

PlateSpin® Protect 11.1

Benutzerhandbuch

März 2015

www.netiq.com/documentation

Rechtliche Hinweise

Lizenzerteilung

Lizenzen für PlateSpin Protect 11.1 können nicht für frühere Versionen von PlateSpin Protect verwendet werden.

Software von Drittanbietern

Weitere Informationen zu Software von Drittanbietern, die in PlateSpin Protect verwendet wird, finden Sie auf der Seite zu *Nutzung und Copyright für Drittanbieterlizenzen in PlateSpin (https://www.netiq.com/documentation/platespin_licensing/platespin_licensing_qs/data/platespin_licensing_qs.html)*.

Inhalt

Info zu NetIQ Corporation

NetIQ ist ein globaler Hersteller von Unternehmenssoftware. Unser Blickpunkt liegt auf drei besonderen Herausforderungen, die Sie in Ihrer Umgebung meistern müssen: Änderungen, Komplexität und Risiken. Unser Ziel ist es, Sie dabei zu unterstützen.

Unser Standpunkt

Sich an Änderungen anzupassen und Komplexität und Risiken zu beherrschen ist nichts Neues

Unter den verschiedenen Herausforderungen, denen Sie gegenüberstehen, beeinflussen diese drei Punkte sicherlich am meisten Ihre Möglichkeiten, Ihre physikalischen, virtuellen und Cloud-Umgebungen sicher zu messen, zu überwachen und zu verwalten.

Kritische Geschäftsservices schneller und besser bereitstellen

Wir sind davon überzeugt, dass IT-Organisationen über eine möglichst große Kontrolle verfügen müssen, um eine zeitgerechte und kostenwirksame Servicebereitstellung zu ermöglichen. Der von Änderungen und Komplexität ausgehende, kontinuierliche Druck steigt ständig, weil sich die Unternehmen ständig ändern und die erforderlichen Technologien zur Verwaltung der Änderungen immer komplexer werden.

Unsere Philosophie

Intelligente Lösungen entwickeln, nicht einfach Software

Damit Sie jederzeit die Kontrolle behalten, informieren wir uns zunächst über sämtliche Aspekte der Szenarien, in denen IT-Unternehmen wie Ihres tagtäglich arbeiten. Nur so können wir praxistaugliche, intelligente IT-Lösungen entwickeln, die nachweisbar messbare Ergebnisse liefern. Und das ist für uns wesentlich bereichernder, als einfach eine Software zu verkaufen.

Ihr Erfolg ist unsere Leidenschaft

Ihr Erfolg ist der Wegweiser für unser Geschäft. Wir wissen, dass Sie IT-Lösungen von der Produktkonzeption bis hin zur Bereitstellung suchen, die richtig funktionieren und nahtlos mit Ihren vorhandenen Investitionen integriert werden können. Sie benötigen fortlaufenden Support, Schulungen nach der Bereitstellung und jemanden, mit dem Sie unkompliziert arbeiten können. Ihr Erfolg ist auch unser Erfolg.

Unsere Lösungen

- Identitäts- und Zugriffsregelung
- Zugriffsverwaltung
- Sicherheitsverwaltung
- System- und Anwendungsverwaltung

* Workload-Management
* Serviceverwaltung

Anfragen an den Vertriebssupport

Bei Fragen zu Produkten, Preisen und Funktionen wenden Sie sich an Ihren Händler vor Ort. Wenn dies nicht möglich ist, wenden Sie sich an unser Vertriebssupport-Team.

Weltweit:	www.netiq.com/about_netiq/officelocations.asp
Vereinigte Staaten und Kanada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Kontakt zum technischen Support

Bei spezifischen Produktproblemen wenden Sie sich bitte an unseren technischen Support.

Weltweit:	www.netiq.com/support/contactinfo.asp
Nord- und Südamerika:	1-713-418-5555
Europa, Naher Osten und Afrika:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Im *Handbuch zum technischen Support* (https://www.netiq.com/Support/process.asp#_Maintenance_Programs_and) finden Sie weitere Informationen zu den Services und Verfahren des NetIQ-Supports.

Kontakt zum Dokumentationssupport

Wir möchten Ihnen stets eine nützliche, aussagekräftige Dokumentation an die Hand geben. Die Dokumentation für dieses Produkt steht auf der Website der PlateSpin Protect-Dokumentation (https://www.netiq.com/documentation/platespin-protect/)im HTML- und PDF-Format zur Verfügung.

Wenn Sie uns einen Verbesserungsvorschlag in Bezug auf die Dokumentation mitteilen möchten, nutzen Sie die Schaltfläche **comment on this topic** (Kommentar zum Thema abgeben), die unten auf jeder Seite der HTML-Version unserer Dokumentation verfügbar ist. Sie können Verbesserungsvorschläge auch per Email an Documentation-Feedback@netiq.com senden. Wir freuen uns auf Ihre Rückmeldung.

Kontakt zur Online-Benutzer-Community

NetIQ Communities, die NetIQ-Online-Community, ist ein Netzwerk zur Zusammenarbeit mit anderen NetIQ-Benutzern und -Experten. NetIQ Communities bietet Ihnen aktuelle Informationen, nützliche Links zu hilfreichen Ressourcen und Kontakt zu NetIQ-Experten, damit Sie über alle Voraussetzungen verfügen, um das meiste aus den IT-Investitionen zu holen, auf die Sie sich verlassen. Weitere Informationen hierzu finden Sie im Internet unter http://community.netiq.com.

Info zu diesem Handbuch und zur Bibliothek

Dieses *Benutzerhandbuch* enthält Informationen zur Verwendung von PlateSpin Protect. Dieses Handbuch bietet allgemeine Informationen, einen Überblick über die Benutzeroberfläche sowie Schritt-für-Schritt-Anweisungen für häufig anfallende Aufgaben Ferner sind Terminologiedefinitionen und Informationen zur Fehlerbehebung enthalten.

Zielgruppe

Dieses Handbuch ist für IT-Mitarbeiter wie beispielsweise Rechenzentrumsadministratoren und -operatoren vorgesehen, die PlateSpin Protect in Workload-Schutzprojekten verwenden.

Informationen in der Bibliothek

Die Bibliothek für dieses Produkt steht im HTML- und PDF-Format auf der Website der PlateSpin Protect-Dokumentation (https://www.netiq.com/documentation/platespin-protect/) bereit. Die Online-Dokumentation steht in den Sprachen Chinesisch (vereinfacht), Chinesisch (traditionell), Deutsch, Englisch, Französisch, Japanisch und Spanisch zur Verfügung.

Die PlateSpin Protect-Bibliothek enthält folgende Informationsressourcen:

Versionshinweise

Informationen zu neuen Funktionen und Verbesserungen in der Version sowie zu bekannten Problemen.

Installations- und Aufrüstungshandbuch

Ausführliche Informationen für die Planung und Installation sowie für die Aufrüstung der Software.

Benutzerhandbuch

Allgemeine Informationen, Überblick der Benutzeroberflächen und Schritt-für-Schritt-Anweisungen für häufig anfallende Aufgaben.

Hilfe

Kontextabhängige Informationen und Schritt-für-Schritt-Anweisungen für häufig anfallende Aufgaben in der Benutzeroberfläche.

Zusätzliche Ressourcen

Wir empfehlen Ihnen, die folgenden zusätzlichen Online-Ressourcen zu nutzen:

- PlateSpin Protect-Forum: (https://forums.netiq.com/forumdisplay.php?59-Platespin-Protect) Web-Community mit Produktbenutzern, in der Sie die Funktionen von NetIQ-Produkten diskutieren und Ratschläge von anderen Produktbenutzern erhalten können.
- PlateSpin Protect-Produktseite: (https://www.netiq.com/products/protect/) Webgestützte Produktbroschüre mit Informationen zu den Funktionen, Angaben zum Bestellvorgang, technischen Daten, häufig gestellten Fragen und zahlreichen Ressourcen wie Videos und Whitepaper.
- NetIQ User Community: (https://www.netiq.com/communities/) Eine webbasierte Community mit verschiedenen Diskussionsthemen.
- NetIQ Support-Knowledgebase: (https://www.netiq.com/support/kb/) eine Sammlung ausführlicher technischer Artikel.
- NetIQ Support-Foren: (https://forums.netiq.com/forum.php) Website, auf der die Produktbenutzer die Funktionen von NetIQ-Produkten diskutieren und Ratschläge von anderen Produktbenutzern erhalten können.
- MyNetIQ: (https://www.netiq.com/f/mynetiq/) Website mit Informationen und Services, beispielsweise Zugriff auf wichtige Whitepaper, Webcast-Registrierung und Testversionen zum Herunterladen.

1 Produktübersicht

Dieser Abschnitt enthält folgende Informationen:

1.1 Informationen zu PlateSpin Protect

PlateSpin Protect ist eine Software zur Geschäftskontinuität und Wiederherstellung im Katastrophenfall, die physische und virtuelle Workloads (Betriebssysteme, Middleware und Daten) anhand von Virtualisierungstechniken schützt. Im Fall eines Ausfalls oder einer Katastrophe am Produktionsserver, kann eine virtualisierte Reproduktion eines Workloads im Ziel *container* (einem VM-Host) aktiviert werden und weiterhin normal ausgeführt werden bis die Produktionsumgebung wiederhergestellt ist.

PlateSpin Protect ermöglicht Ihnen Folgendes:

- Schnelle Wiederherstellung von Workloads nach einem Fehler
- Schutz von mehreren Workloads gleichzeitig
- Testen des Failover-Workloads ohne Ihre Produktionsumgebung zu beeinträchtigen
- Failback für Failover-Workloads durchführen, entweder auf ihre ursprünglichen oder auf völlig neue Infrastrukturen, ob physische oder virtuelle
- Unterstützung externer Speicherlösungen, z. B. SANs

1.2 Unterstützte Konfigurationen

PlateSpin Protect unterstützt Server-Workloads zum Schutz der meisten Hauptversionen der Betriebssysteme Microsoft Windows, SUSE Linux Enterprise und Red Hat Enterprise Linux. In diesem Abschnitt werden die unterstützten Plattformkonfigurationen beschrieben.

1.2.1 Unterstützte Windows-Workloads

PlateSpin Protect unterstützt Workloads für die meisten Versionen von Microsoft Windows. Eine Liste der unterstützten Windows-Versionen finden Sie unter Tabelle 1-1.

Sowohl die Reproduktionen auf Dateiebene als auch die auf Blockebene werden unterstützt, mit bestimmten Einschränkungen. Weitere Informationen hierzu finden Sie unter Abschnitt 5.4, „Datenübertragung“, auf Seite 83.

Tabelle 1-1 *Unterstützte Windows-Workloads*

Betriebssystem	Notizen
Serverklassen-Workloads	
Windows Server 2012 R2 Windows Server 2012	
Windows Server 2008 R2 (64-Bit) Windows Server 2008 (64-Bit) Windows Server 2008, aktuelles SP (32-Bit)	Einschließlich Domänencontroller(DC)- und Small Business Server(SBS)-Editionen
Windows Server 2003 R2 (64-Bit) Windows Server 2003 R2 (32-Bit) Windows Server 2003 mit aktuellem SP (64-Bit) Windows Server 2003 mit aktuellem SP (32-Bit)	Windows 2003 erfordert SP1 oder höher für die blockbasierte Reproduktion.
Windows 2008 R2 Server-basiertes Microsoft-Failovercluster	
Hypervisor-Klassen-Workloads	
Windows Server 2012 mit Hyper-V-Rolle	
Arbeitsstationsklassen-Workloads	
Windows 8.1 Windows 8	**WARNUNG:** Sie müssen den Energiesparplan **Hohe Leistung** an der Windows 8-Quelle auswählen, damit die Workload-Failover- und -Failback-Funktion korrekt funktioniert. So konfigurieren Sie diesen Energiesparplan in der Windows-Systemsteuerung: 1. Wählen Sie **Alle Systemsteuerungselemente > Energieoptionen**. 2. Wählen Sie im Dialogfeld **Energiesparplan wählen oder anpassen** die Optionen **Weitere Energiesparpläne einblenden > Hohe Leistung**. 3. Schließen Sie die Systemsteuerung.

Unterstützte Windows-Dateisysteme

PlateSpin Protect unterstützt auf allen unterstützten Windows-Systemen ausschließlich das NTFS-Dateisystem.

Unterstützte Windows-Cluster

PlateSpin Protect unterstützt den Schutz der Geschäftsdienste eines Microsoft Windows-Clusters. Folgende Cluster-Technologien werden unterstützt:

- Windows 2008 R2 Server-basiertes Microsoft-Failovercluster

Weitere Informationen zum Schutz von Workloads in einem Cluster finden Sie unter „Schützen von Windows-Clustern“, auf Seite 93.

Unterstützte internationale Versionen

PlateSpin Protect unterstützt Versionen von Microsoft Windows in den Sprachen Französisch, Deutsch, Japanisch, Chinesisch (traditionell) und Chinesisch (vereinfacht).

TIPP: Weitere internationale Versionen werden eingeschränkt unterstützt; beispielweise kann die Aktualisierung von Systemdateien in anderen Sprachen erfolgen.

Unterstützung für Workload-Firmware (UEFI und BIOS)

PlateSpin Protect spiegelt die Microsoft-Unterstützung für UEFI- oder BIOS-basierte Windows-Workloads wider. Es überträgt Workloads (sowohl Block- als auch Dateitransfers werden unterstützt) von der Quelle an das Ziel und erzwingt die unterstützte Firmware für die entsprechende Quelle bzw. das Ziel und die Zielbetriebssysteme. Dies gilt auch für das Failback auf einen physischen Computer. Sobald ein Übergang (Failover oder Failback) zwischen UEFI- und BIOS-Systemen eingeleitet wird, analysiert Protect diesen Übergang und Sie erhalten eine Mitteilung über dessen Gültigkeit.

HINWEIS: Wenn Sie einen UEFI-basierten Workload schützen und während des gesamten Lebenszyklus des geschützten Workloads denselben Firmware-Startmodus nutzen möchten, muss ein Container mit vSphere 5.0 (oder höher) als Ziel verwendet werden.

Die folgenden Beispiele zeigen das Protect-Verhalten beim Schutz und Failback zwischen UEFI- und BIOS-basierten Systemen:

- Beim Übertragen eines UEFI-basierten Workloads auf einen Container mit VMware vSphere 4.*x* (der UEFI nicht unterstützt) führt Protect zum Zeitpunkt des Failbacks einen Übergang der UEFI-Firmware des Workloads zur BIOS-Firmware durch. Wenn dann das Failback auf einem UEFI-basierten physischen Computer ausgewählt wird, kehrt Protect den Firmware-Übergang von BIOS zu UEFI wieder um.
- Wenn Sie versuchen, ein Failback eines geschützten Windows 2003-Workloads auf einen UEFI-gestützten physischen Computer vorzunehmen, analysiert Protect die Auswahl und informiert Sie, dass dieser Vorgang nicht gültig ist. (Der Firmware-Übergang von BIOS zu UEFI wird nicht unterstützt, da Windows 2003 den UEFI-Startmodus nicht unterstützt).
- Beim Schützen eines UEFI-basierten Ursprungs auf einem BIOS-basierten Ziel migriert Protect die Startlaufwerke des UEFI-Systems (bislang GPT) zu MBR-Laufwerken. Bei einem Failback dieses BIOS-Workloads auf einen UEFI-basierten physischen Computer werden die Startlaufwerke wieder zu GPT zurückkonvertiert.

Unterstützung für komplexe Workload-Festplattenpartitionierung

PlateSpin Protect unterstützt die GPT-Partitionierung von Festplatten für Windows-Workloads. Die vollständige Reproduktion wird für bis zu 57 Partitionen oder Volumes auf einer einzigen Festplatte unterstützt.

1.2.2 Unterstützte Linux-Workloads

PlateSpin Protect unterstützt eine Reihe von Linux-Distributionen. Eine Liste der unterstützten Windows-Versionen finden Sie in Tabelle 1-2.

***Tabelle 1-2** Unterstützte Linux-Workloads*

Betriebssystem	Notizen
Linux-Serverklassen-Workloads	
Red Hat Enterprise Linux (RHEL) 7	Nur blockbasierte Übertragung. Umfasst das XFS-Dateisystem.
RHEL 6.2	Nur blockbasierte Übertragung.
RHEL 5.0-5.5, 6.0	Nur blockbasierte Übertragung.
RHEL 5.6-5.8, 6.3	Nur blockbasierte Übertragung. Sie müssen das PlateSpin-Modul `blkwatch` kompilieren, bevor Sie diese Workloads inventarisieren.
RHEL 4 (32-Bit)	Nur blockbasierte Übertragung.
SUSE Linux Enterprise Server (SLES) 9, 10, 11 (SP1, SP 2, SP 3)	**HINWEIS:** Die Kernel-Version 3.0.13 von SLES 11 SP 3 wird nicht unterstützt. Rüsten Sie auf die Kernel-Version 3.0.27 oder höher auf, bevor Sie den Workload inventarisieren.
Novell Open Enterprise Server (OES) 11, SP1 und SP2	**HINWEIS:** Die Standard-Kernel-Version 3.0.13 von SLES 11 SP 2 wird nicht unterstützt. Rüsten Sie auf die Kernel-Version 3.0.27 oder höher auf, bevor Sie den Workload inventarisieren. Nur blockbasierte Übertragung.
Oracle Enterprise Linux (OEL)	Gleiche Unterstützung wie für Workloads, die RHEL ausführen.
CentOS 7	Nur blockbasierte Übertragung. **HINWEIS:** CentOS wird nur für den experimentellen Gebrauch unterstützt.

Unterstützte Linux-Dateisysteme

PlateSpin Protect unterstützt die Dateisysteme EXT2, EXT3, EXT4, REISERFS, XFS (RHEL-7-Workloads) und NSS (OES-11-Workloads) jeweils nur mit blockbasierter Übertragung.

HINWEIS: Verschlüsselte Workload-Volumes auf dem Ursprung werden auf dem virtuellen Failover-Computer entschlüsselt.

Unterstützung für Workload-Firmware (UEFI und BIOS)

PlateSpin Protect unterstützt Benutzeroberflächen mit UEFI- und BIOS-Firmware.

Unterstützung für komplexe Workload-Festplattenpartitionierung

PlateSpin Protect unterstützt die GPT-Partitionierung von Festplatten für Linux-Workloads. Die vollständige Reproduktion wird für bis zu 57 Partitionen oder Volumes auf einer einzigen Festplatte unterstützt.

Anforderung eines `blkwatch`-Treibers

Die Reproduktion von geschützten Linux-Workloads erfolgt auf Blockebene. Für die PlateSpin Protect-Software ist ein `blkwatch`-Treiber erforderlich, der für die zu schützende Linux-Distribution kompiliert wurde. Eine Liste der Distributionen, die den `blkwatch`-Treiber enthalten, finden Sie unter Anhang A, „Von Protect unterstützte Linux-Distributionen“, auf Seite 125.

Wenn die Distribution den `blkwatch`-Treiber nicht enthält, können Sie einen benutzerdefinierten Treiber erstellen. Führen Sie dazu die im Wissensdatenbankartikel 7005873 beschriebenen Schritte aus.

1.2.3 Unterstützte VM-Container

Ein Container ist eine Schutz-Infrastruktur, die als Host für die regelmäßig aktualisierte Reproduktion eines geschützten Workloads agiert. Diese Infrastruktur kann entweder ein VMware ESXi-Server oder ein VMware DRS-Cluster sein.

Tabelle 1-3 *Plattformen, die als VM-Container unterstützt werden*

Container	Haftnotizen
VMware ESXi 5.5 (GA2, Update 2)	◆ Unterstützt als Schutz- und Failback-Container ◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) ◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 5.5-Servern bestehen und kann nur von vCenter 5.5 verwaltet werden.
VMware ESXi 5.1 (GA2, Update 2)	◆ Unterstützt als Schutz- und Failback-Container ◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) ◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 5.1-Servern bestehen und kann nur von vCenter 5.1 verwaltet werden.
VMware ESXi 4.1 (GA2, Update 3)	◆ Unterstützt als Schutz- und Failback-Container ◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) ◆ Als VM-Container darf der DRS-Cluster nur aus ESXi 4.1-Servern bestehen und kann nur von vCenter 4.1 verwaltet werden.

Darüber hinaus unterstützt PlateSpin Protect die Mehrmandantenfähigkeit in VMware. Mehrere Protect-Server können gemeinsam ein VMware-Cluster-Backend nutzen. Weitere Informationen hierzu finden Sie unter Abschnitt 5.3, „Einrichten der Protect-Mehrmandantenfähigkeit auf VMWare“, auf Seite 76.

1.2.4 Unterstützte System-Firmware

PlateSpin Protect unterstützt Benutzeroberflächen mit UEFI- und BIOS-Firmware.

Auf Windows-Systemen spiegelt PlateSpin Protect die Microsoft-Unterstützung für UEFI wider. Weitere Informationen finden Sie unter Unterstützung für Workload-Firmware (UEFI und BIOS) in Abschnitt 1.2.1, „Unterstützte Windows-Workloads“, auf Seite 14.

1.3 Sicherheit und Datenschutz

PlateSpin Protect stellt Ihnen eine Reihe von Funktionen zur Verfügung, mit denen Sie Ihre Daten schützen und die Sicherheit Ihres Systems erhöhen können.

1.3.1 Sicherheit der Workload-Daten bei der Übertragung

Sie können den Workload-Schutz so konfigurieren, dass die Daten verschlüsselt werden, um die Übertragung Ihrer Workload-Daten sicherer zu machen. Wenn die Verschlüsselung aktiviert ist, werden über das Netzwerk reproduzierte Daten unter Verwendung von AES (Advanced Encryption Standard) verschlüsselt.

Falls erforderlich, können Sie Ihren PlateSpin-Server für die Verwendung eines Datenverschlüsselungs-Algorithmus konfigurieren, der FIPS (Federal Information Processing Standards, Publication 140-2) entspricht. Weitere Informationen finden Sie unter „Aktivieren der Unterstützung für FIPS-konforme Datenverschlüsselungs-Algorithmen (optional)“ im *PlateSpin Protect Installations- und Aufrüstungshandbuch*.

Sie können die Verschlüsselung für jeden Workload einzeln aktivieren oder deaktivieren. Weitere Informationen hierzu finden Sie unter „Workload-Schutz-Details“, auf Seite 62.

1.3.2 Sicherheit der Client-Server-Kommunikation

Da durch die PlateSpin-Serverinstallation SSL auf dem PlateSpin-Server-Host aktiviert wird, ist die sichere Datenübertragung zwischen Ihrem Webbrowser und dem PlateSpin-Server bereits auf HTTPS (Hypertext Transfer Protocol Secure) konfiguriert. Bei der Installation wird auch ein eigensigniertes Zertifikat hinzugefügt, falls keine gültigen Zertifikate gefunden werden.

1.3.3 Sicherheit von Berechtigungsnachweisen

Der Berechtigungsnachweis, den Sie für den Zugriff auf verschiedene Systeme (z. B. Workloads und Failback-Ziele) verwenden, wird in der PlateSpin -Datenbank gespeichert und unterliegt daher denselben Sicherheitsmechanismen, die Sie für den PlateSpin Protect-Server-Host implementiert haben.

Darüber hinaus sind Berechtigungsnachweise in der Diagnose enthalten, die für berechtigte Benutzer zugänglich ist. Sie sollten sicherstellen, dass Workload-Schutz-Projekte von befugten Mitarbeitern bearbeitet werden.

1.3.4 Benutzerautorisierung und -authentifizierung

PlateSpin Protect bietet einen umfassenden und sicheren Benutzerautorisierungs- und -authentifizierungsmechanismus, der auf Benutzerrollen basiert und den Anwendungszugriff sowie die Aktionen steuert, die Benutzer ausführen können. Weitere Informationen hierzu finden Sie in Abschnitt 2.2, „Einrichten der Benutzerautorisierung und -authentifizierung“, auf Seite 25.

1.3.5 Windows-Authentifizierung für die Microsoft SQL Server-Datenbank

PlateSpin Protect bietet die Möglichkeit, den Zugriff auf die Microsoft SQL Server-Datenbank über die Windows-Authentifizierung vorzunehmen. Weitere Informationen hierzu finden Sie unter Abschnitt 2.3.4, „Zugriffs- und Kommunikationsanforderungen für die Windows-Authentifizierung bei der Microsoft SQL Server-Datenbank“, auf Seite 32.

1.3.6 Zusätzliche Sicherheitsverbesserungen

Im Wissensdatenbankartikel 7015818 finden Sie Informationen, wie Sie die Angreifbarkeit durch potenzielle POODLE-Angriffe (Padding Oracle On Downgraded Legacy Encryption) von Ihren PlateSpin-Servern beseitigen.

1.4 Leistung

1.4.1 Allgemeines zu Produktleistungsmerkmalen

Die Leistungsmerkmale Ihres PlateSpin Protect-Produkts sind von einer Reihe von Faktoren abhängig, darunter:

- Hardware- und Softwareprofile Ihrer Ursprungs-Workloads
- Hardware- und Softwareprofile Ihrer Ziel-Container
- Hardware- und Softwareprofil Ihres PlateSpin-Server-Hosts
- Eigenschaften Ihrer Netzwerkbandbreite, -konfiguration und -bedingungen
- Die Anzahl der geschützten Workloads
- Die Anzahl der Volumes unter Schutz
- Die Größe der Volumes unter Schutz
- Dateidichte (Anzahl der Dateien pro Kapazitätseinheit) auf den Volumes des Ursprungs-Workloads
- Ursprungs-E/A-Ebenen (die Auslastung Ihrer Workloads)
- Die Anzahl der gleichzeitigen Reproduktionen

- Ob die Datenverschlüsselung aktiviert oder deaktiviert ist
- Ob die Datenkomprimierung aktiviert oder deaktiviert ist

Bei umfangreichen Workload-Schutz-Plänen sollten Sie einen Testschutz eines typischen Workloads und einige Reproduktionen durchführen und das Ergebnis als Benchmark verwenden, wobei Sie Ihre Metriken während des gesamten Projekts regelmäßig feineinstellen sollten.

1.4.2 Datenkomprimierung

Falls erforderlich, kann PlateSpin Protect die Workload-Daten vor der Übertragung über das Netzwerk komprimieren. So können Sie die Gesamtmenge der während Reproduktionen übertragenen Daten verringern.

Die Komprimierungsverhältnisse hängen von der Art der Dateien auf den Volumes eines Ursprungs-Workloads ab und können von 0,9 (100 MB Daten komprimiert auf 90 MB) bis etwa 0,5 (100 MB komprimiert auf 50 MB) variieren.

HINWEIS: Die Datenkomprimierung verwendet die Prozessorleistung des Ursprungs-Workloads.

Die Datenkomprimierung kann für jeden Workload einzeln oder auf einer Schutzebene konfiguriert werden. Weitere Informationen hierzu finden Sie in „Schutzebenen“, auf Seite 84.

1.4.3 Bandbreitendrosselung

In PlateSpin Protect können Sie die Menge an Netzwerkbandbreite, die im Verlauf eines Workload-Schutzes durch die direkte Ursprung-zu-Ziel-Kommunikation verbraucht wird, steuern. Sie können für jeden Schutzplan eine Durchsatzrate festlegen. Dies verhindert, dass Reproduktionsverkehr Ihr Produktionsnetzwerk verstopft, und verringert die Gesamtlast Ihres PlateSpin-Servers.

Die Bandbreitendrosselung kann für jeden Workload einzeln konfiguriert werden oder auf einer Schutzebene. Weitere Informationen hierzu finden Sie in „Schutzebenen“, auf Seite 84.

1.4.4 RPO-, RTO- und TTO-Spezifikationen

- **Angestrebter Wiederherstellungszeitpunkt (RPO):** Beschreibt die akzeptable Menge an Datenverlust, gemessen in Zeit. Der RPO ermittelt sich aus der Zeit zwischen den inkrementellen Reproduktionen eines geschützten Workloads und wird vom aktuellen Nutzungsumfang von PlateSpin Protect, der Rate und dem Ausmaß von Änderungen im Workload sowie von der Netzwerkgeschwindigkeit und dem gewählten Reproduktionszeitplan beeinflusst.
- **Angestrebte Wiederherstellungszeit (RTO):** Beschreibt die Zeit, die für einen Failover-Vorgang (einen Failover-Workload in den Online-Modus versetzen, um einen geschützten Produktions-Workload vorübergehend zu ersetzen) benötigt wird.

  Die für einen Failover eines Workloads auf dessen virtuelle Reproduktion benötigte RTO wird von der Zeit beeinflusst, die für das Konfigurieren und Ausführen des Failover-Vorgangs benötigt wird (10 bis 45 Minuten). Weitere Informationen hierzu finden Sie in „Failover“, auf Seite 66.
- **Angestrebte Testzeit (TTO):** Beschreibt die Zeit, die zum Testen des Wiederherstellungsplans benötigt wird, damit der Dienst erfolgreich wiederhergestellt werden kann.

  Verwenden Sie die Funktion **Failover testen**, um verschiedene Szenarien zu durchlaufen und Vergleichsdaten zu generieren. Weitere Informationen hierzu finden Sie unter „Verwenden der Funktion „Failover testen““, auf Seite 67.

Zu den Faktoren, die Auswirkungen auf den RPO sowie die RTO und TTO haben, gehört die Anzahl der erforderlichen gleichzeitigen Failover-Vorgänge. Ein einzelner Failover-Workload verfügt über mehr Arbeitsspeicher und CPU-Ressourcen als mehrere Failover-Workloads, die sich die Ressourcen der ihnen zugrunde liegenden Infrastruktur teilen.

Führen Sie zum Ermitteln der durchschnittlichen Failover-Zeiten für Workloads in Ihrer Umgebung Test-Failovers zu unterschiedlichen Zeiten durch und verwenden Sie sie als Vergleichsdaten in Ihren Gesamtwiederherstellungsplänen. Weitere Informationen hierzu finden Sie unter „Generieren von Workload- und Workload-Schutz-Berichten“, auf Seite 55.

1.4.5 Skalierbarkeit

Die Skalierbarkeit hängt von den folgenden Hauptmerkmalen Ihres PlateSpin Protect-Produkts ab:

- **Workloads pro Server:** Die Anzahl der Workloads pro PlateSpin-Server kann zwischen 10 und 50 variieren. Dies hängt von verschiedenen Faktoren ab, z. B. Ihren RPO-Anforderungen und den Hardware-Eigenschaften des Server-Hosts.
- **Schutz pro Container:** Der maximale Schutz pro Container basiert auf den VMware-Spezifikationen bezüglich der maximalen Anzahl an unterstützten VMs pro ESXi-Host (ist aber nicht identisch). Weitere Faktoren sind die Wiederherstellungsstatistik (einschließlich der gleichzeitigen Reproduktionen und Failovers) sowie die Händlerspezifikationen für die Hardware.

Sie sollten Tests durchführen, Ihre Kapazitätszahlen stufenweise anpassen und sie zur Bestimmung der maximalen Skalierbarkeit verwenden.

2 PlateSpin Protect-Anwendungskonfiguration

Dieser Abschnitt enthält Informationen zu folgenden Themen:

2.1 Produktlizenzierung

Dieser Abschnitt enthält Informationen für die Aktivierung der PlateSpin Protect-Software.

2.1.1 Abrufen eines Lizenzaktivierungscodes

Für die Produktlizenzierung benötigen Sie einen Lizenzaktivierungscode. Falls Sie nicht über einen Lizenzaktivierungscode verfügen, können Sie diesen beim Customer Center (http://www.netiq.com/customercenter/) anfordern. Sie erhalten dann eine Email mit einem Lizenzaktivierungscode.

Wenn Sie sich zum ersten Mal bei PlateSpin Protect anmelden, wird der Browser automatisch zur Seite für die Lizenzaktivierung umgeleitet. Sie haben zwei Möglichkeiten, um Ihre Produktlizenz zu aktivieren: Online-Lizenzaktivierung oder Offline-Lizenzaktivierung.

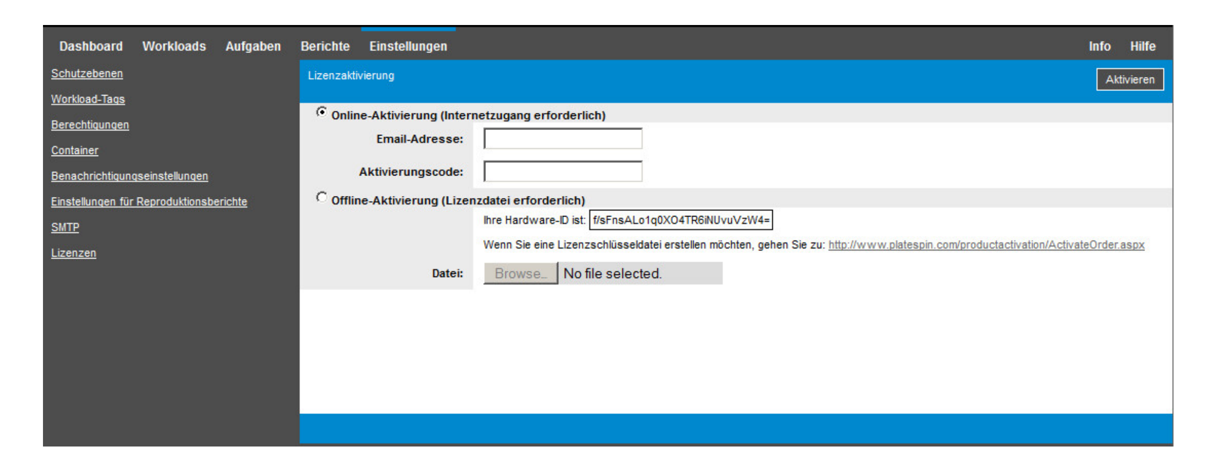
2.1.2 Online-Lizenzaktivierung

Für die Online-Aktivierung von PlateSpin Protect benötigen Sie einen Internetzugang.

HINWEIS: HTTP-Proxys können während der Online-Aktivierung Fehler verursachen. Benutzern in Umgebungen mit einem HTTP-Proxy wird die Offline-Aktivierung empfohlen.

So richten Sie die Online-Lizenzaktivierung ein:

1. Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen > Lizenzen > Lizenz hinzufügen**. Die Seite „Lizenzaktivierung“ wird angezeigt.



2 Wählen Sie **Online-Aktivierung**, geben Sie die Email-Adresse, die Sie auch bei der Auftragserteilung angegeben haben, sowie den erhaltenen Aktivierungscode an, und klicken Sie auf **Aktivieren**.

Das System ruft die erforderliche Lizenz über das Internet ab und aktiviert das Produkt.

2.1.3 Offline-Lizenzaktivierung

Für die Offline-Aktivierung erhalten Sie einen Lizenzschlüssel über das Internet, indem Sie einen Computer mit Internetzugang verwenden.

HINWEIS: Sie müssen über ein Novell-Konto verfügen, um einen Lizenzschlüssel abrufen zu können. Wenn Sie bereits PlateSpin-Kunde sind und kein Customer Center-Konto besitzen, müssen Sie zunächst eines erstellen. Verwenden Sie Ihren bestehenden PlateSpin-Benutzernamen (eine gültige bei PlateSpin registrierte Email-Adresse) als Benutzernamen für Ihr Customer Center-Konto.

---

1 Klicken Sie auf **Einstellungen** > **Lizenz** und dann auf **Lizenz hinzufügen**. Die Seite „Lizenzaktivierung“ wird angezeigt.

2 Wählen Sie **Offline-Aktivierung** aus und kopieren Sie die angezeigte Hardware-ID.

3 Navigieren Sie in einem Webbrowser auf einem Computer mit Internetanschluss zur PlateSpin-Produktaktivierungs-Website (http://www.platespin.com/productactivation/ActivateOrder.aspx). Melden Sie sich mit Ihrem Novell-Benutzernamen und Ihrem Passwort an.

4 Füllen Sie die entsprechenden Felder aus:

- Den erhaltenen Aktivierungscode
- Die bei der Auftragserteilung angegebene Email-Adresse
- Die in Schritt 2 kopierte Hardware-ID

5 Klicken Sie auf **Aktivieren**.

Das System generiert eine Lizenzschlüsseldatei und fordert Sie auf, diese zu speichern.

6 Speichern Sie die generierte Lizenzschlüsseldatei, übertragen Sie sie zum Produkt-Host, der über keine Internet-Konnektivität verfügt, und aktivieren Sie damit das Produkt.

2.2 Einrichten der Benutzerautorisierung und -authentifizierung

Der Abschnitt enthält folgende Informationen:

2.2.1 Info über die Benutzerautorisierung und -authentifizierung von PlateSpin Protect

Der Benutzerautorisierungs- und authentifizierungsmechanismus von PlateSpin Protect basiert auf Benutzerrollen und steuert den Anwendungszugriff sowie die Aktionen, die Benutzer ausführen können. Diesem Mechanismus liegen die Integrierte Windows-Authentifizierung (IWA) und deren Interaktion mit den Internetinformationsdiensten (IIS) zugrunde.

Der rollenbasierte Zugriffsmechanismus bietet Ihnen verschiedene Möglichkeiten, die Autorisierung und Authentifizierung von Benutzern zu implementieren:

- Anwendungszugriff auf bestimmte Benutzer beschränken
- Bestimmte Aktionen nur bestimmten Benutzern erlauben
- Jedem Benutzer Zugriff auf bestimmte Workloads gewähren, um die durch die zugewiesene Rolle definierten Aktionen durchzuführen

Jede PlateSpin Protect-Instanz verfügt auf der Betriebssystemebene über folgende Benutzergruppen, die entsprechende funktionale Rollen definieren:

- **Workload-Schutz-Administratoren:** Besitzen unbegrenzten Zugriff auf alle Funktionen der Anwendung. Ein lokaler Administrator ist implizit Teil dieser Gruppe.
- **Workload-Schutz-Hauptbenutzer:** Besitzen Zugriff auf die meisten Funktionen der Anwendung, jedoch mit einigen Einschränkungen, z. B. hinsichtlich des Änderns von Systemeinstellungen für die Lizenzierung und Sicherheit.
- **Workload-Schutz-Operatoren:** Besitzen Zugriff auf einen eingeschränkten Teil der Systemfunktionen, und zwar jene, die für die alltägliche Nutzung ausreichen.

Wenn ein Benutzer versucht, eine Verbindung mit PlateSpin Protect herzustellen, wird der über den Browser angegebene Berechtigungsnachweis vom IIS geprüft. Wenn der Benutzer keiner der Workload-Schutz-Rollen angehört, wird die Verbindung verweigert.

Tabelle 2-1 *Details zu Workload-Schutz-Rollen und -Berechtigungen*

Details zu Workload-Schutz-Rollen	Administratoren	Power-Benutzer	Operatoren
Workload hinzufügen	Zulässig	Zulässig	Verweigert
Workload entfernen	Zulässig	Zulässig	Verweigert
Schutz konfigurieren	Zulässig	Zulässig	Verweigert

Details zu Workload-Schutz-Rollen	Administratoren	Power-Benutzer	Operatoren
Reproduktion vorbereiten	Zulässig	Zulässig	Verweigert
(Voll-)Reproduktion ausführen	Zulässig	Zulässig	Zulässig
Inkrementelle Reproduktion ausführen	Zulässig	Zulässig	Zulässig
Zeitplan unterbrechen/wieder aufnehmen	Zulässig	Zulässig	Zulässig
Failover testen	Zulässig	Zulässig	Zulässig
Failover	Zulässig	Zulässig	Zulässig
Failover abbrechen	Zulässig	Zulässig	Zulässig
Abbrechen	Zulässig	Zulässig	Zulässig
Zurückweisen (Aufgabe)	Zulässig	Zulässig	Zulässig
Einstellungen (Alle)	Zulässig	Verweigert	Verweigert
Berichte/Diagnose ausführen	Zulässig	Zulässig	Zulässig
Failback	Zulässig	Verweigert	Verweigert
Erneut schützen	Zulässig	Zulässig	Verweigert

Darüber hinaus bietet die PlateSpin Protect-Software einen auf *Sicherheitsgruppen* basierenden Mechanismus, der definiert, welche Benutzer auf welche Workloads im Workload-Inventar von PlateSpin Protect zugreifen dürfen.

Das Einrichten eines ordnungsgemäßen rollenbasierten Zugriffs auf PlateSpin Protect umfasst zwei Aufgaben:

1. Hinzufügen von Benutzern zu den erforderlichen Benutzergruppen, zu denen Sie unter Tabelle 2-1 (in Ihrer Windows-Dokumentation) detaillierte Informationen finden können.
2. Erstellen von Sicherheitsgruppen auf Anwendungsebene, die diese Benutzer bestimmten Workloads zuordnen (weitere Informationen finden Sie unter „Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen“, auf Seite 28).

2.2.2 Verwalten von PlateSpin Protect-Zugriff und -Berechtigungen

Die folgenden Abschnitte enthalten weitere Informationen:

- „Hinzufügen von PlateSpin Protect-Benutzern“, auf Seite 27
- „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 27

Hinzufügen von PlateSpin Protect-Benutzern

Gehen Sie wie in diesem Abschnitt beschrieben vor, um einen neuen PlateSpin Protect-Benutzer hinzuzufügen.

Falls Sie einem auf dem PlateSpin Server-Host vorhandenen Benutzern bestimmte Rollenberechtigungen gewähren möchten, lesen Sie bitte unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 27 weiter.

1. Öffnen Sie auf dem PlateSpin-Server-Host die Systemkonsole „Lokale Benutzer und Gruppen“ (**Start** > **Ausführen** > `lusrmgr.msc` > **Eingabetaste**).
2. Klicken Sie mit der rechten Maustaste auf den Knoten **Benutzer**, wählen Sie **Neuer Benutzer** aus, geben Sie die erforderlichen Details an und klicken Sie auf **Erstellen**.

Jetzt können Sie dem gerade erstellten Benutzer eine Workload-Schutz-Rolle zuweisen. Weitere Informationen hierzu finden Sie unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 27.

Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer

Bevor Sie einem Benutzer eine Rolle zuweisen, ermitteln Sie, welche Berechtigungen für diesen Benutzer am Besten geeignet sind. Weitere Informationen hierzu finden Sie unter Tabelle 2-1, „Details zu Workload-Schutz-Rollen und -Berechtigungen“, auf Seite 25.

1. Öffnen Sie auf dem PlateSpin-Server-Host die Systemkonsole „Lokale Benutzer und Gruppen“ (**Start** > **Ausführen** > `lusrmgr.msc` > **Eingabetaste**).
2. Klicken Sie auf den Knoten **Benutzer** und doppelklicken Sie im rechten Fenster auf den erforderlichen Benutzer.
3. Klicken Sie in der Registerkarte **Mitglied von** auf **Hinzufügen**, suchen Sie nach der erforderlichen Workload-Schutz-Gruppe und weisen Sie sie dem Benutzer zu.

Es kann einige Minuten dauern, bis die Änderung wirksam wird. Zur manuellen Anwendung der Änderungen müssen Sie den Server mit der ausführbaren Datei `RestartPlateSpinServer.exe` neu starten.

So starten Sie den Webserver neu:

1. Wechseln Sie in das Unterverzeichnis `bin\RestartPlateSpinServer` des PlateSpin-Servers.
2. Doppelklicken Sie auf die Programmdatei `RestartPlateSpinServer.exe`.

   Es wird ein Befehlszeilenfenster geöffnet, in dem Sie aufgefordert werden, den Vorgang zu bestätigen.
3. Geben Sie `Y` ein und drücken Sie die `Eingabetaste`.

Jetzt können Sie diesen Benutzer einer PlateSpin Protect-Sicherheitsgruppe hinzufügen und ihm eine angegebene Sammlung von Workloads zuweisen. Weitere Informationen hierzu finden Sie unter „Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen“, auf Seite 28.

2.2.3 Verwalten von PlateSpin Protect-Sicherheitsgruppen und -Workload-Berechtigungen

PlateSpin Protect bietet auf der Anwendungsebene einen genauer definierten Zugriffsmechanismus, der es bestimmten Benutzern erlaubt, bestimmte Workload-Schutz-Aufgaben für angegebene Workloads durchzuführen. Dies wird durch die Einrichtung von *Sicherheitsgruppen* erreicht.

1 Weisen Sie einem PlateSpin Protect-Benutzer die Workload-Schutz-Rolle zu, deren Berechtigungen am besten für die Rolle dieses Benutzers in Ihrer Organisation geeignet sind. Weitere Informationen hierzu finden Sie unter „Zuweisung einer Workload-Schutz-Rolle an einen PlateSpin Protect-Benutzer“, auf Seite 27.

2 Greifen Sie als Administrator auf der PlateSpin Protect-Weboberfläche auf PlateSpin Protect zu, und klicken Sie auf **Einstellungen > Berechtigungen**.

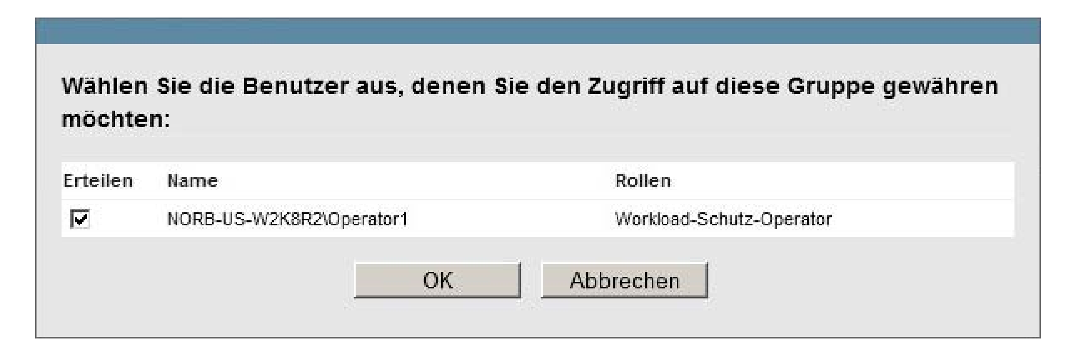
   Die Seite „Sicherheitsgruppen“ wird angezeigt:

3 Klicken Sie auf **Sicherheitsgruppe erstellen**.

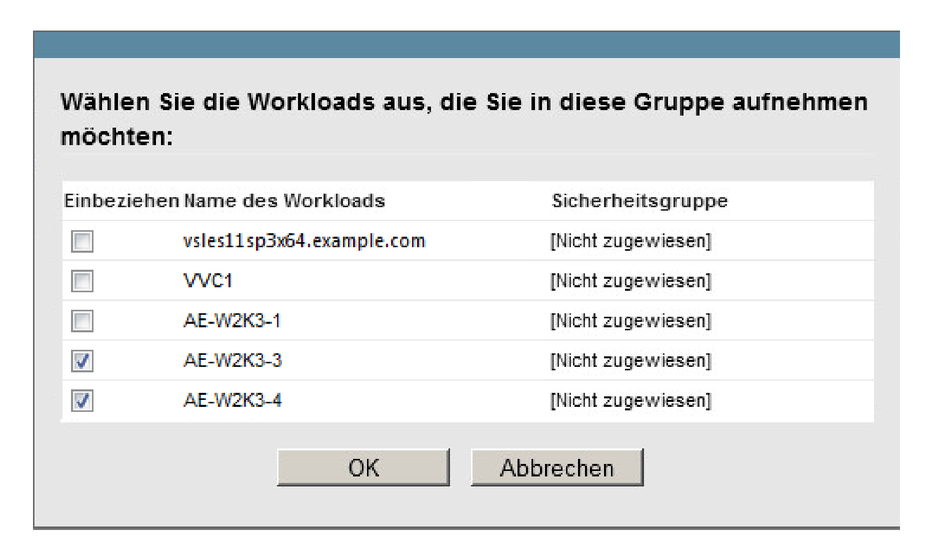
4 Geben Sie im Feld **Name der Sicherheitsgruppe** einen Namen für Ihre Sicherheitsgruppe ein.

5 Klicken Sie auf **Benutzer hinzufügen** und wählen Sie die erforderlichen Benutzer für diese Sicherheitsgruppe aus.

   Wenn Sie einen PlateSpin Protect-Benutzer hinzufügen möchten, der kürzlich zum PlateSpin Protect-Server-Host hinzugefügt wurde, wird er möglicherweise nicht sofort auf der Benutzeroberfläche angezeigt. Klicken Sie in diesem Fall auf **Benutzerkonten aktualisieren**.



6 Klicken Sie auf **Workload hinzufügen** und wählen Sie die erforderlichen Workloads aus:



Nur die Benutzer in dieser Sicherheitsgruppe haben Zugriff auf die ausgewählten Workloads.

7 Klicken Sie auf **Erstellen**.

Die Seite wird neu geladen und zeigt Ihre neue Gruppe in der Liste der Sicherheitsgruppen an.

Wenn Sie eine Sicherheitsgruppe bearbeiten möchten, klicken Sie in der Liste der Sicherheitsgruppen auf ihren Namen.

2.3 Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk

Dieser Abschnitt enthält folgende Informationen:

2.3.1 Anforderungen für geöffnete Ports für PlateSpin-Server-Hosts

Die folgenden Anforderungen gelten für geöffnete Ports für PlateSpin-Server-Hosts.

Tabelle 2-2 *Anforderungen für geöffnete Ports für PlateSpin-Server-Hosts*

Port (Standard)	Anmerkungen
TCP 80	Für HTTP-Kommunikation
TCP 443	Für die HTTPS-Kommunikation (wenn SSL aktiviert ist)

2.3.2 Zugriffs- und Kommunikationsanforderungen für Workloads

Im folgenden Abschnitt werden die Software-, Netzwerk- und Firewall-Anforderungen für Workloads beschrieben, die mithilfe von PlateSpin Protect geschützt werden sollen.

Tabelle 2-3 *Zugriffs- und Kommunikationsanforderungen für Workloads*

Workload-Typ	Voraussetzungen	Erforderliche Ports (Standards)
Alle Workloads	Ping-Unterstützung (ICMP-Echoanfrage und -antwort)	

Workload-Typ	Voraussetzungen	Erforderliche Ports (Standards)
Alle Windows-Workloads	Microsoft .NET Framework Version 2.0 oder 3.5 SP1	
Windows 7; Windows Server 2008; Windows Vista	◆ Integrierter `Administrator`- oder Domänen-Administrator-Kontoberechtigungsnachweis (die Mitgliedschaft in der lokalen Administratorgruppe reicht nicht aus). Unter Vista muss das Konto aktiviert sein (es ist standardmäßig deaktiviert). ◆ Die Windows-Firewall, die so konfiguriert ist, dass sie die **Datei- und Druckerfreigabe** zulässt. Verwenden Sie eine der folgenden Optionen: ◆ **Option 1 mit der Windows-Firewall:** Verwenden Sie das grundlegende Systemsteuerungselement **Windows-Firewall** (`firewell.cpl`) und wählen Sie in der Liste der Ausnahmen die Option **Datei- und Druckerfreigabe** aus. - ODER - ◆ **Option 2 mit der Firewall mit erweiterter Sicherheit:** Verwenden Sie das Dienstprogramm Windows-Firewall mit erweiterter Sicherheit (`wf.msc`), bei dem die folgenden **Eingangsregeln** aktiviert und auf `Zulassen` festgelegt sind: ◆ **Datei- und Druckerfreigabe (Echoanforderung Alt+0150 ICMPv4In)** ◆ **Datei- und Druckerfreigabe (Echoanforderung Alt+0150 ICMPv6In)** ◆ **Datei- und Druckerfreigabe (NB-Datagramm eingehend)** ◆ **Datei- und Druckerfreigabe (NB-Name eingehend)** ◆ **Datei- und Druckerfreigabe (NB-Sitzung eingehend)** ◆ **Datei- und Druckerfreigabe (SMB eingehend)** ◆ **Datei- und Druckerfreigabe (Spoolerdienst Alt+0150 RPC)** ◆ **Datei- und Druckerfreigabe (Spoolerdienst – RPC-EPMAP)**	TCP 3725 NetBIOS 137 – 139 SMB (TCP 139, 445 und UDP 137, 138) TCP 135/445
Windows Server 2003 (mit SP1 Standard, SP2 Enterprise und R2 SP2 Enterprise)	**HINWEIS:** Nach dem Aktivieren der erforderlichen Anschlüsse aktivieren Sie die PlateSpin-Remote-Verwaltung mit dem folgenden Befehl an der Server-Eingabeaufforderung: `netsh firewall set service RemoteAdmin enable` Weitere Informationen zum Befehl „netsh“ finden Sie im Microsoft TechNet-Artikel *Das Befehlszeilenprogramm „Netsh“* (http://technet.microsoft.com/en-us/library/cc785383%28v=ws.10%29.aspx).	◆ **TCP:** 3725, 135, 139, 445 ◆ **UDP:** 137, 138, 139

Workload-Typ	Voraussetzungen	Erforderliche Ports (Standards)
Windows Server 2000; Windows XP	◆ Installierte Windows Management Instrumentation (WMI) WMI (RPC/DCOM) kann die TCP-Ports 135 und 445 sowie zufällig oder dynamisch zugewiesene Ports oberhalb von 1024 verwenden. Wenn beim Hinzufügen des Workloads Probleme auftreten, erwägen Sie, den Workload vorübergehend in ein DMZ zu stellen oder die durch die Firewall geschützten Ports vorübergehend zu öffnen, während Sie den Workload zu PlateSpin Protect hinzufügen. Weitere Informationen, z. B. eine Anleitung für das Beschränken des Portbereichs für DCOM und RPC, finden Sie in den folgenden technischen Artikeln von Microsoft. ◆ *Verwenden von DCOM mit Firewalls* (http://msdn.microsoft.com/en-us/library/ms809327.aspx) ◆ *Konfigurieren der dynamischen RPC-Port-Zuordnung für die Verwendung mit Firewalls* (http://support.microsoft.com/default.aspx?scid=kb;en-us;154596) ◆ *Konfigurieren von DCOM für die Verwendung mit einer NAT-basierten Firewall* (http://support.microsoft.com/kb/248809)	TCP 3725 NetBIOS 137 – 139 SMB (TCP 139, 445 und UDP 137, 138) RPC (TCP 135)
Alle Linux-Workloads	Secure Shell (SSH)-Server	TCP 22, 3725

2.3.3 Zugriffs- und Kommunikationsanforderungen für Container

Die folgenden Software-, Netzwerk- und Firewall-Anforderungen gelten für die unterstützten Workload-Container.

***Tabelle 2-4** Zugriffs- und Kommunikationsanforderungen für Container*

System	Voraussetzungen	Erforderliche Ports (Standards)
Alle Container	Ping-Funktion (ICMP-Echoanfrage und -antwort).	
VMware ESX/ESXi 4.1 VMware ESXi 5.0	◆ VMware-Konto mit Administratorrolle ◆ VMware Web-Services-API und Dateiverwaltungs-API	HTTPS (TCP 443)
vCenter Server	Dem zugreifenden Benutzer müssen die erforderlichen Rollen und Berechtigungen zugewiesen sein. Weitere Informationen hierzu finden Sie in der entsprechenden VMware-Dokumentation.	HTTPS (TCP 443)

2.3.4 Zugriffs- und Kommunikationsanforderungen für die Windows-Authentifizierung bei der Microsoft SQL Server-Datenbank

PlateSpin Protect bietet die Möglichkeit, den Zugriff auf die Microsoft SQL Server-Datenbank über die Windows-Authentifizierung vorzunehmen. Für die Authentifizierung müssen Sie die Active Directory-Einstellungen konfigurieren und Ports in der Firewall öffnen.

So aktivieren Sie die Windows-Authentifizierung bei der SQL-Datenbank:

1. Konfigurieren Sie Microsoft SQL Server so, dass sowohl TCP/IP-Verbindungen als auch Named-Pipe-Verbindungen zugelassen werden.
2. (Bedingt) Falls der Zugriff auf die Microsoft SQL Server-Datenbank über die Windows-Authentifizierung erfolgen soll, müssen Sie Folgendes in Active Directory konfigurieren:
   - Sie müssen den Microsoft SQL Server-Datenbankserver in die Domäne aufnehmen.
   - Sie benötigen zwei Domänenbenutzerkonten für die PlateSpin Protect-Installation.
     - **Ein Domänenbenutzer mit dem `sysadmin`-Rollensatz:** Mit diesem Benutzer werden Datenbanken, Tabellen und andere Schemaobjekte erstellt.
     - **PlateSpin-Service-Benutzer:** Der Servicebenutzer kann ein Domänenbenutzer mit niedrigen Rechten in der Domäne sein. Allerdings muss der Servicebenutzer als lokaler Administrator des PlateSpin Protect-Servers fungieren und diese Berechtigung vor Beginn der Installation erhalten.

       Wenn das Passwort des Windows-Benutzers geändert wird, müssen Sie das Passwort für den PlateSpin-Service-Benutzer und für den IIS-Anwendungspool aktualisieren. Verwenden Sie daher nach Möglichkeit einen Windows-Benutzer, dessen Passwort niemals ausläuft.

   HINWEIS: Beim Aufrüsten wird das Anmelden bei der SQL Server-Datenbank über die Windows-Authentifizierung nicht unterstützt.

   ---
3. Zur Unterstützung der Authentifizierung auf dem SQL-Server öffnen Sie die folgenden Ports in der Firewall:
   - **Ports 49152-65535/TCP:** Datenverkehr für RPC für LSA, SAM, Netlogon (*) zulassen.
   - **Port 1433/TCP:** Datenverkehr für Microsoft SQL Server zulassen.
   - **Benutzerdefinierte Ports:** Wenn Sie SQL Server für einen benutzerdefinierten TCP-P konfigurieren, müssen Sie diesen Port in der Firewall öffnen.

   HINWEIS: Falls Sie keine dynamischen Ports nutzen, müssen Sie den dedizierten Port im Feld **Datenbankserver** angeben.

   ---
4. (Bedingt) Sollen dedizierte Ports für PlateSpin Protect verwendet werden, müssen Sie die Ports in der Firewall öffnen:

   4a Legen Sie auf dem Datenbankserver fest, welche Ports geöffnet werden müssen:

   4a1 Wählen Sie im SQL Server-Konfigurationsmanager die Option **Protokolle für SQLExpress > TCP/IP**, klicken Sie mit der rechten Maustaste, und wählen Sie **Eigenschaften**.

   4a2 Wählen Sie im Dialogfeld die Registerkarte **IP-Adressen**.

4a3 Wenn für **TCP-Port** oder **Dynamische TCP-Ports** ein Wert ungleich 0 festgelegt ist, öffnen Sie unter **IP/Alle** (oder unter dem gewünschten Protokoll) die gewünschten Ports in der Firewall. Über diese Ports stellen Sie eine Verbindung zum SQL-Server her.

Wenn für das Feld **Dynamische TCP-Ports** beispielsweise der Wert 60664 festgelegt ist und für das Feld **TCP-Port** der Wert 1555, müssen Sie entsprechend die Ports 60664 und 1555 in den Firewall-Regeln auf dem SQL-Server aktivieren.

4b Öffnen Sie die Ports in der Firewall.

HINWEIS: Falls eine Wertemenge für dynamische Ports vorliegt, wird Ihr Server unter Umständen nicht in der Liste der SQL-Server aufgeführt, wenn Sie auf **Durchsuchen** klicken. In diesem Fall müssen Sie den Server manuell im Eingabefeld **Datenbankserver** der PlateSpin Protect-Installation angeben.

Wenn der Servername beispielsweise `MYSQLSERVER` und der Name der Datenbankinstanz `SQLEXPRESS` lautet und für den dynamischen Port der dedizierte Port `60664` festgelegt ist, geben Sie den folgenden Text ein, und wählen Sie dann den gewünschten Authentifizierungstyp aus:

```
MEINSQLSERVER\SQLEXPRESS,60664
```

Sie müssen die Ports in der Firewall öffnen.

2.3.5 Schutz über öffentliche und private Netzwerke durch NAT

In einigen Fällen kann sich ein Ursprung, ein Ziel oder PlateSpin Protect selbst in einem internen (privaten) Netzwerk hinter einem NAT-Gerät (Network Address Translator) befinden, wodurch eine Kommunikation mit dem Gegenstück während des Schutzes nicht möglich ist.

PlateSpin Protect ermöglicht Ihnen, dieses Problem zu umgehen, je nachdem, welcher der folgenden Hosts sich hinter dem NAT-Gerät befindet:

- **PlateSpin-Server:** Fügen Sie die diesem Host zugewiesenen zusätzlichen IP-Adressen zum *PlateSpin Server Configuration*-Werkzeug Ihres Servers hinzu. Weitere Informationen hierzu finden Sie unter „Konfigurieren der Anwendung zum Funktionieren über NAT“, auf Seite 34.
- **Ziel-Container:** Wenn Sie versuchen, einen Container zu ermitteln, z. B. VMware ESX, geben Sie die öffentlichen (oder externen) IP-Adressen dieses Hosts in den Parametern für die Ermittlung an.
- **Workload:** Geben Sie bei dem Versuch, einen Workload hinzuzufügen, die öffentliche (interne) IP-Adresse dieses Workloads in den Ermittlungsparametern an.
- **Failover-VM:** Bei einem Failback können Sie eine alternative IP-Adresse für den Failover-Workload in Failback-Details (Workload an VM) (Seite 70) angeben.
- **Failback-Ziel:** Wenn Sie bei dem Versuch ein Failback-Ziel zu registrieren dazu aufgefordert werden, die IP-Adresse des PlateSpin-Servers anzugeben, müssen Sie entweder die lokale Adresse des Protect-Server-Hosts angeben oder eine seiner öffentlichen (externen) Adressen, die im *PlateSpin Server Configuration*-Werkzeug des Servers aufgezeichnet wurden (weitere Informationen hierzu finden Sie oben unter „*PlateSpin-Server*“).

Konfigurieren der Anwendung zum Funktionieren über NAT

Damit der PlateSpin Forge-Server über alle NAT-aktivierten Umgebungen funktioniert, müssen Sie zusätzliche IP-Adressen Ihres PlateSpin Forge-Servers in der Datenbank im *PlateSpin Server Configuration*-Werkzeug aufzeichnen, die der Server beim Starten liest.

Weitere Informationen zum Aktualisierungsvorgang finden Sie unter „Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern“, auf Seite 39.

2.3.6 Außerkraftsetzen der Standard-Bash-Shell zum Ausführen von Befehlen auf Linux-Workloads

Standardmäßig verwendet der PlateSpin-Server bei der Ausführung von Befehlen auf einem Linux-basierten Workload die `/bin/bash`-Shell.

Falls erforderlich, können Sie die Standard-Shell außer Kraft setzen, indem Sie den entsprechenden Registry-Schlüssel auf dem PlateSpin-Server ändern.

Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7010676.

2.3.7 Anforderungen für VMware DRS-Cluster als Container

Um ein gültiges Schutzziel sein zu können, muss Ihr VMware DRS-Cluster dem Satz der (inventarisierten) Container als VMware-Cluster hinzugefügt werden. Sie sollten nicht versuchen, einen DRS-Cluster als einen Satz von individuellen ESX-Servern hinzuzufügen. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern (Schutzziele)“, auf Seite 59.

Außerdem muss Ihr VMware-Cluster die folgenden Konfigurationsanforderungen erfüllen:

- DRS ist aktiviert und auf `Teilweise automatisiert` oder auf `Vollautomatisch` gesetzt sein.
- Mindestens eine Datenablage muss für alle ESX-Server im VMware-Cluster freigegeben sein.
- Mindestens ein vSwitch und eine virtuelle Portgruppe bzw. ein dezentraler vNetwork-Schalter ist für alle ESX-Server im VMware-Cluster gleich.
- Die Failover-Workloads (VMs) für jeden Schutzvertrag werden ausschließlich in Datenablagen, vSwitches und virtuellen Portgruppen platziert, die über alle ESX-Server im VMware-Cluster gemeinsam genutzt werden.

2.4 Konfigurieren von PlateSpin Protect-Standardoptionen

Dieser Abschnitt enthält folgende Informationen:

2.4.1 Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten

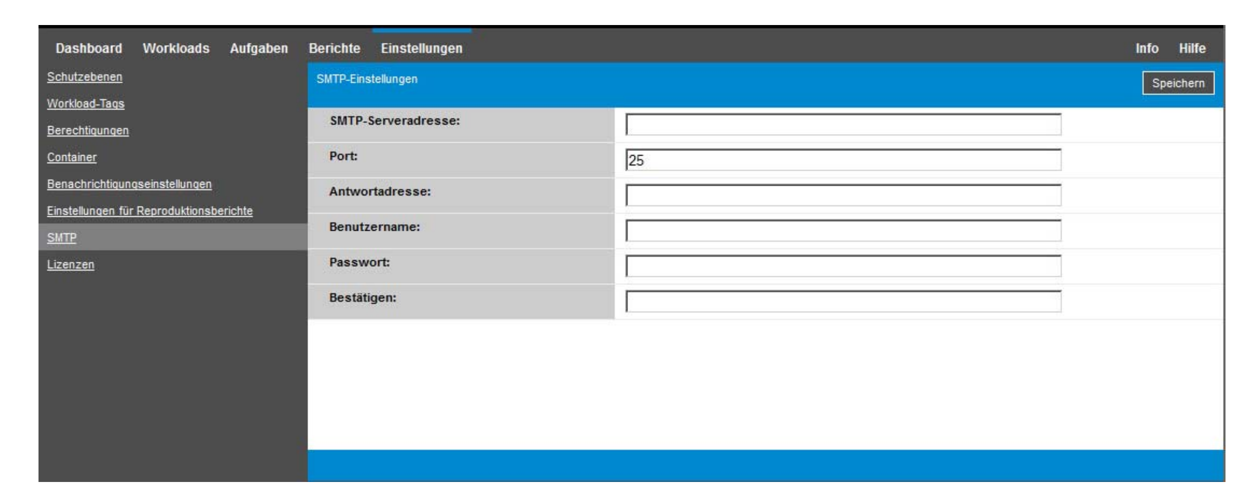
Sie können PlateSpin Protect so konfigurieren, dass es automatisch Benachrichtigungen zu Ereignissen und Reproduktionsberichte an angegebene Email-Adressen sendet. Für diese Funktion ist es erforderlich, dass Sie zuerst einen gültigen SMTP-Server für PlateSpin Protect angeben.

- „SMTP-Konfiguration", auf Seite 35
- „Einrichten automatischer Ereignisbenachrichtigungen per Email", auf Seite 35
- „Einrichten automatischer Reproduktionsberichte per Email", auf Seite 37

SMTP-Konfiguration

Konfigurieren Sie auf der PlateSpin Protect-Weboberfläche die SMTP-Einstellungen für den Server, der zum Zustellen von Email-Benachrichtigungen zu Ereignissen und Reproduktionsberichten verwendet wird.

Abbildung 2-1 *SMTP-Einstellungen (Simple Mail Transfer Protocol)*



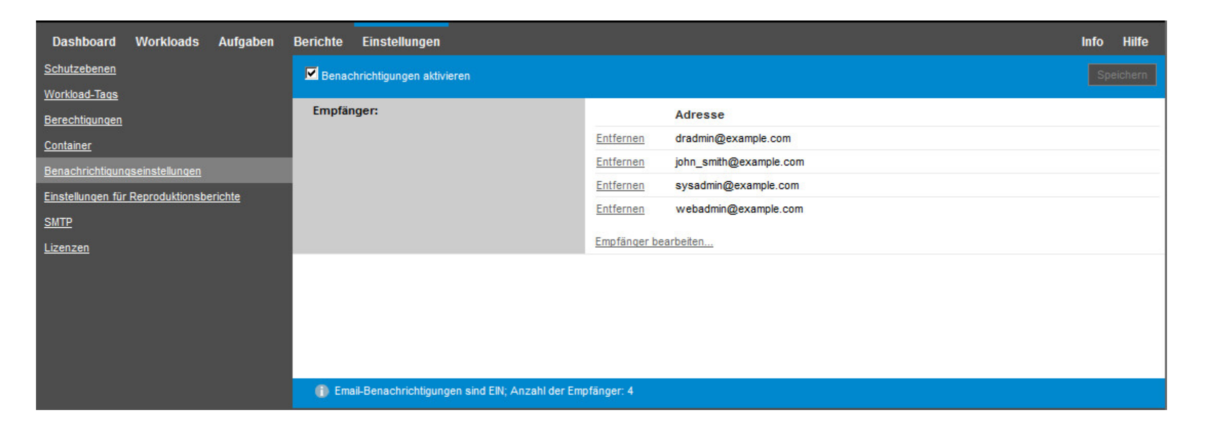
So konfigurieren Sie die SMTP-Einstellungen:

1. Klicken Sie auf Ihrer PlateSpin Protect-Weboberfläche auf **Einstellungen > SMTP**.
2. Geben Sie die **Adresse** und den **Port** (Standardport ist 25) Ihres SMTP-Servers sowie eine **Antwortadresse** für den Empfang von Email-Benachrichtigungen zu Ereignissen und zum Fortschritt an.
3. Geben Sie den **Benutzernamen** und das **Passwort** ein. Bestätigen Sie anschließend das Passwort.
4. Klicken Sie auf **Speichern**.

Einrichten automatischer Ereignisbenachrichtigungen per Email

1. Richten Sie einen SMTP-Server für PlateSpin Protect ein. Weitere Informationen hierzu finden Sie in „SMTP-Konfiguration", auf Seite 35.
2. Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen > Benachrichtigungseinstellungen**.
3. Wählen Sie die Option **Benachrichtigungen aktivieren**.

4 Klicken Sie auf **Empfänger bearbeiten**, geben Sie die erforderlichen Email-Adressen getrennt durch Kommas ein und klicken Sie anschließend auf **OK**.



5 Klicken Sie auf **Speichern**.

Klicken Sie zum Löschen aufgelisteter Email-Adressen auf **Löschen** neben den zu entfernenden Adressen.

Die in Tabelle 2-5 genannten Ereignisarten können Email-Benachrichtigungen auslösen, wenn die Benachrichtigungsfunktion konfiguriert ist. Die Ereignisse werden stets in das Systemanwendungs-Ereignisprotokoll mit den Protokolleintragsarten „Warnmeldung“, „Fehler“ und „Informationen“ eingetragen.

HINWEIS: Die Ereignisprotokolleinträge besitzen eindeutige IDs, die sich jedoch in künftigen Hauptversionen durchaus ändern können.

***Tabelle 2-5** Ereignistypen nach Protokolleintragsarten*

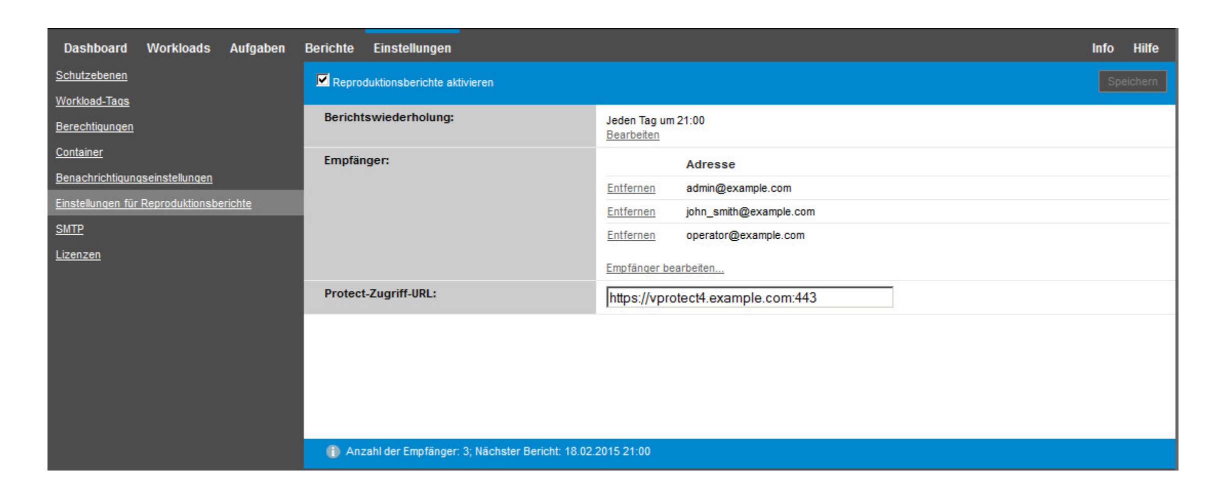
Ereignisarten	Anmerkungen
Protokolleintragsart: Warnmeldung	
`FullReplicationMissed`	Ähnlich dem Ereignis `Inkrementelle Reproduktion verpasst.`
`IncrementalReplicationMissed`	Wird generiert, wenn Folgendes zutrifft: ◆ Eine Reproduktion wird manuell angehalten, wenn eine geplante inkrementelle Reproduktion fällig ist. ◆ Das System versucht, eine geplante inkrementelle Reproduktion auszuführen, während gerade eine manuell ausgelöste Reproduktion stattfindet. ◆ Das System stellt fest, dass das Ziel nicht über genügend freien Speicherplatz verfügt.

Ereignisarten	Anmerkungen
`WorkloadOfflineDetected`	Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor online war, nun offline ist. Betrifft Workloads, deren Schutzvertragsstatus nicht **Unterbrochen** lautet.
Protokolleintragsart: Fehler	
`FailoverFailed`	
`FullReplicationFailed`	
`IncrementalReplicationFailed`	
`PrepareFailoverFailed`	
Protokolleintragsart: Informationen	
`FailoverCompleted`	
`FullReplicationCompleted`	
`IncrementalReplicationCompleted`	
`PrepareFailoverCompleted`	
`TestFailoverCompleted`	Wird generiert, wenn ein Failover-Test-Vorgang manuell als ordnungsgemäß durchgeführt oder als Fehler gekennzeichnet wird.
`WorkloadOnlineDetected`	Wird generiert, wenn das System erkennt, dass ein Workload, der zuvor offline war, nun online ist. Betrifft Workloads, deren Schutzvertragsstatus nicht **Unterbrochen** lautet.

Einrichten automatischer Reproduktionsberichte per Email

Führen Sie folgende Schritte aus, um PlateSpin Protect so einzurichten, dass es automatisch Reproduktionsberichte per Email sendet:

1. Richten Sie einen SMTP-Server für PlateSpin Protect ein. Weitere Informationen hierzu finden Sie in SMTP-Konfiguration (Seite 35).
2. Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen > Email > Einstellungen für Reproduktionsberichte**.
3. Wählen Sie die Option **Reproduktionsberichte aktivieren**.
4. Klicken Sie im Abschnitt **Berichtswiederholung** auf **Konfigurieren** und geben Sie das erforderliche Wiederholungsmuster für die Berichte an.
5. Klicken Sie im Abschnitt **Empfänger** auf **Empfänger bearbeiten**, geben Sie die erforderlichen Email-Adressen getrennt durch Kommas ein und klicken Sie anschließend auf **OK**.



6 (Optional) Geben Sie im Abschnitt **Protect-Zugriff-URL** eine nicht standardmäßige URL für Ihren PlateSpin-Server ein (z. B. wenn Ihr PlateSpin-Server-Host mehrere Netzwerkkarten hat oder sich hinter einem NAT-Server befindet). Diese URL hat Einfluss auf den Titel des Berichts und auf die Funktionalität für den Zugriff auf relevante Inhalte auf dem Server über Hyperlinks in Email-Berichten.

7 Klicken Sie auf **Speichern**.

Informationen zu anderen Arten von Berichten, die Sie jederzeit generieren können, finden Sie unter „Generieren von Workload- und Workload-Schutz-Berichten“, auf Seite 55.

2.4.2 Einrichtung der Sprache bei internationalen Versionen von PlateSpin Protect

PlateSpin Protect bietet Unterstützung von Landessprachen (NLS, National Language Support) für Chinesisch (vereinfacht), Chinesisch (traditionell), Französisch, Deutsch und Japanisch.

Zur Verwendung der PlateSpin Protect-Weboberfläche und der integrierten Hilfe in einer dieser Sprachen muss die entsprechende Sprache in Ihrem Webbrowser hinzugefügt und an die erste Position der Rangfolge gesetzt werden:

1 Rufen Sie im Webbrowser die Spracheinstellung auf:
   - **Internet Explorer:** Klicken Sie auf **Extras > Internetoptionen > Registerkarte „Allgemein“** > **Sprachen**.
   - **Firefox:** Klicken Sie auf **Extras > Einstellungen > Registerkarte „Inhalt“** > **Sprachen**.

2 Fügen Sie die gewünschte Sprache hinzu und setzen Sie sie an die oberste Position in der Liste.

3 Speichern Sie die Einstellungen und starten Sie anschließend die Client-Anwendung, indem Sie eine Verbindung zu Ihrem PlateSpin-Server herstellen. Weitere Informationen hierzu finden Sie unter „Starten der PlateSpin Protect-Weboberfläche“, auf Seite 47.

HINWEIS: (Für Benutzer der chinesischen Versionen) Der Versuch, über einen Browser ohne spezifische chinesische Version eine Verbindung zum PlateSpin Server herzustellen, kann zu Webserverfehlern führen. Verwenden Sie für den ordnungsgemäßen Betrieb die Konfigurationseinstellungen des Browsers, um eine spezifische chinesische Spracheinstellung hinzuzufügen (`Chinesisch [zh-cn]` oder `Chinesisch [zh-tw]`). Verwenden Sie die kulturneutrale Spracheinstellung `Chinesisch [zh]` nicht.

Die Sprache eines geringen Anteils der vom PlateSpin-Server generierten Systemmeldungen hängt von der Oberflächensprache des Betriebssystems ab, die auf Ihrem PlateSpin Server-Host ausgewählt ist:

1. Rufen Sie Ihren PlateSpin Server-Host auf.
2. Starten Sie das Applet für die Regions- und Sprachoptionen (klicken Sie auf **Start > Ausführen**, geben Sie `intl.cpl` ein und drücken Sie die Eingabetaste) und klicken Sie anschließend auf die Registerkarte **Sprachen** (Windows Server 2003) bzw. **Tastaturen und Sprachen** (Windows Server 2008).
3. Installieren Sie das erforderliche Sprachpaket, sofern es noch nicht installiert ist. Möglicherweise benötigen Sie Zugriff auf die Installationsmedien Ihres Betriebssystems.
4. Wählen Sie die erforderliche Sprache als Oberflächensprache des Betriebssystems aus. Wenn eine entsprechende Aufforderung angezeigt wird, melden Sie sich ab oder starten Sie das System neu.

2.4.3 Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern

Bestimmte Aspekte des Verhaltens des PlateSpin-Servers werden anhand von Konfigurationsparametern gesteuert, die Sie auf einer Konfigurationswebseite mit Ihrem PlateSpin-Server-Host (`https://`*`Ihr_PlateSpin-Server`*`/platespinconfiguration/`) festlegen.

Normalerweise brauchen Sie diese Einstellungen nicht zu ändern, es sei denn, der PlateSpin-Support rät Ihnen dazu. In diesem Abschnitt werden einige häufig vorkommende Fälle zusammen mit Informationen zur erforderlichen Prozedur aufgeführt.

Gehen Sie wie folgt vor, um Konfigurationsparameter zu ändern oder anzuwenden:

1. Öffnen Sie `https://`*`Ihr_PlateSpin-Server`*`/platespinconfiguration/` in einem beliebigen Webbrowser.
2. Suchen Sie den gewünschten Serverparameter und ändern Sie dessen Wert.
3. Speichern Sie die Einstellungen und schließen Sie die Seite.

Nach Änderungen im Konfigurationswerkzeug ist kein Neustart des Computers oder der Dienste erforderlich.

In den nachfolgenden Themen finden Sie Informationen zu verschiedenen Situationen, in denen Sie das Produktverhalten mithilfe eines XML-Konfigurationswerts ändern müssen.

- „Optimieren des Datentransfers über WAN-Verbindungen“, auf Seite 40
- „Einrichten der Unterstützung für SRM“, auf Seite 42

HINWEIS: Über die Konfigurationsseite können Sie außerdem die Weboberfläche an das Markenbild anpassen. Weitere Informationen finden Sie in Anhang C, „Anpassen der PlateSpin Protect-Weboberfläche an das Markenbild“, auf Seite 129.

Optimieren des Datentransfers über WAN-Verbindungen

Sie können die Datentransferleistung optimieren und sie für WAN-Verbindungen fein abstimmen. Dazu können Sie die Konfigurationsparameter ändern, die das System anhand der Einstellungen im Konfigurationswerkzeug auf Ihrem PlateSpin-Server-Host liest. Weitere Informationen zu dem generischen Vorgang finden Sie unter „Konfigurieren des Verhaltens des PlateSpin-Servers mithilfe von XML-Konfigurationsparametern“, auf Seite 39.

Verwenden Sie diese Einstellungen zur Optimierung der Datentransfers über ein WAN. Diese globalen Einstellungen gelten für alle dateibasierten und VSS-Reproduktionen.

HINWEIS: Wenn diese Werte geändert werden, können die Reproduktionszeiten in Hochgeschwindigkeits-Netzwerken wie Gigabit Ethernet möglicherweise negativ beeinflusst werden. Wenden Sie sich lieber zuerst an den PlateSpin-Support bevor Sie diese Parameter ändern.

Tabelle 2-6 enthält eine Liste der Konfigurationsparameter, die die Dateiübertragungsgeschwindigkeit mit den Standard- bzw. Höchstwerten steuern. Zum Optimieren der Funktionsfähigkeit in einer WAN-Umgebung mit hoher Latenz können Sie diese Werte nach dem Versuch von Versuch und Irrtum bearbeiten.

Tabelle 2-6 *Standardmäßige und optimierte Konfigurationsparameter für die Dateiübertragung in `https://Ihr_PlateSpin-Server/platespinconfiguration/`*

Parameter	Standardwert	Höchstwert
`AlwaysUseNonVSSFileTransferForWindows2003`	Falsch	
`FileTransferCompressionThreadsCount` Steuert die Anzahl der Threads, die für die Datenkomprimierung auf Paketebene verwendet werden. Diese Einstellung wird ignoriert, wenn die Komprimierung deaktiviert ist. Da die Komprimierung CPU-abhängig ist, kann sich diese Einstellung auf die Arbeitsgeschwindigkeit auswirken.	2	nicht zutreffend
`FileTransferBufferThresholdPercentage` Bestimmt die Mindestdatenmenge, die im Puffer gespeichert wird, bevor neue Netzwerkpakete erstellt und gesendet werden.	10	
`FileTransferKeepAliveTimeOutMilliSec` Gibt an, wie lange mit dem Absenden von Keep-Alive-Meldungen gewartet werden soll, wenn eine TCP-Zeitüberschreitung eingetreten ist.	120000	
`FileTransferLongerThan24HoursSupport`	Wahr	
`FileTransferLowMemoryThresholdInBytes` Bestimmt die Untergrenze für die Speichermenge auf dem Server. (Unterhalb dieser Mindestmenge treten bestimmte Netzwerkverhaltensweisen stärker auf.)	536870912	
`FileTransferMaxBufferSizeForLowMemoryInBytes` Bestimmt die Größe des internen Puffers bei mangelndem Speicherplatz.	5242880	

Parameter	Standardwert	Höchstwert
`FileTransferMaxBufferSizeInBytes` Bestimmt die Größe des internen Puffers für die Speicherung von Paketdaten.	31457280	
`FileTransferMaxPacketSizeInButes` Bestimmt die Größe der größten noch versendbaren Pakete.	1048576	
`FileTransferMinCompressionLimit` Gibt den Schwellwert für die Komprimierung auf Paketebene in Byte an.	0 (deaktiviert)	Max. 65536 (64 KB)
`FileTransferPort`	3725	

`FileTransferSendReceiveBufferSize`
 	
Gibt die Einstellung der TCP/IP-Fenstergröße für Dateiübertragungsverbindungen an. Sie steuert die Anzahl der Byte, die ohne TCP-Acknowledgement gesendet werden. Angabe in Byte.
 	
Wenn der Wert auf 0 (aus) gesetzt wird, wird die Standard-TCP-Fenstergröße (8 KB) verwendet. Geben Sie bei benutzerdefinierten Größen die Größe in Byte an. Verwenden Sie folgende Formel, um den geeigneten Wert zu ermitteln:
 	
((Verbindungsgeschwindigkeit(MB/s)/ 8)*Verzögerung(Sek.))*1000*1000
 	
Beispielsweise wäre die geeignete Puffergröße bei einer 100-Mb/s-Verbindung mit 10 ms Latenz wie folgt:
 	
`(100/8)*0,01 * 1000 * 1000 = 125000 Byte`
	0 (8192 Byte)	Max. 5242880 (5 MB)

`FileTransferSendReceiveBufferSizeLinux` Gibt die Einstellung der TCP/IP-Fenstergröße für Dateiübertragungsverbindungen unter Linux an. Sie steuert die Anzahl der Byte, die ohne TCP-Acknowledgement gesendet werden. Angabe in Byte. Wenn der Wert auf 0 (aus) gesetzt ist, wird die TCP/IP-Fenstergröße für Linux automatisch anhand der Einstellung für `FileTransferSendReceiveBufferSize` berechnet. Sind beide Parameter auf 0 (aus) gesetzt, gilt der Standardwert 248 KB. Geben Sie bei benutzerdefinierten Größen die Größe in Byte an. **HINWEIS:** In früheren Versionen vor PlateSpin Forge 11.1, PlateSpin Protect 11.1 und PlateSpin Migrate 12 mussten Sie diesen Parameter auf die Hälfte des gewünschten Werts einstellen; dies ist nicht mehr erforderlich.	0 (253952 Byte)	
`FileTransferShutDownTimeOutInMinutes`	1090	
`FileTransferTCPTimeOutMilliSec` Legt den Zeitraum für die Zeitüberschreitung für TCP-Senden und TCP-Empfang fest.	30.000	

Parameter	Standardwert	Höchstwert
`PostFileTransferActionsRequiredTimeInMinutes`	60	

Einrichten der Unterstützung für SRM

Workloads, die von PlateSpin Protect reproduziert und vom VMware vCenter Site Recovery Manager (SRM) verwaltet werden, funktionieren nahtlos, wenn Sie die Unterstützung für SRM konfigurieren. Im Rahmen der Konfiguration müssen einige XML-Konfigurationsparameter des PlateSpin Servers geändert werden. Informationen über diese Konfigurationsänderungen finden Sie im Abschnitt 2.4.4, „Konfigurieren der Unterstützung für VMware vCenter Site Recovery Manager“, auf Seite 42.

2.4.4 Konfigurieren der Unterstützung für VMware vCenter Site Recovery Manager

Mit PlateSpin Protect können Sie ihre Workloads lokal schützen und sie mithilfe einer zusätzlichen Methode an einem Remotestandort, wie einem SAN, reproduzieren. Sie können beispielsweise mit VMware vCenter Site Recovery Manager (SRM) eine komplette Datenablage reproduzierter Ziel-VMs an einem Remotestandort reproduzieren. In diesem Fall sind spezifische Konfigurationsschritte erforderlich, um sicherzustellen, dass die Ziel-VMs reproduziert werden können und ordnungsgemäß funktionieren, sobald sie am Remotestandort eingeschaltet werden.

Die Protect-Konfiguration für die Unterstützung für SRM umfasst die folgenden Anpassungen:

- Konfigurieren Sie eine Einstellung, damit die PlateSpin Protect-ISO und -Datenträger in derselben Datenablage gespeichert werden wie die VMware `.vmx`- und `.vmdk`-Dateien.
- Bereiten Sie die PlateSpin Protect-Umgebung auf das Kopieren der VMware Tools auf das Failover-Ziel vor. Dazu müssen einige Dateien manuell erstellt und kopiert werden. Außerdem müssen Konfigurationseinstellungen vorgenommen werden, um den Installationsprozess der VMware Tools zu beschleunigen.

Stellen Sie mit den folgenden Schritten sicher, dass die Workload-Dateien in derselben Datenablage bleiben:

1. Öffnen Sie die Webseite für die Konfiguration. Rufen Sie hierzu in einem Webbrowser die URL `https://`*`Your_PlateSpin_Server`*`/platespinconfiguration/` auf.
2. Navigieren Sie auf der Webseite für die Konfiguration zum Serverparameter `CreatePSFilesInVmDatastore`, und ändern Sie den Wert in `wahr`.

   HINWEIS: Die für das Konfigurieren des Reproduktionsvertrags verantwortliche Person muss sicherstellen, dass für alle VM-Zieldatenträgerdateien dieselbe Datenablage angegeben ist.

3. Speichern Sie die Einstellungen und schließen Sie die Seite.

Die Setup-Pakete für die VMware Tools können während der Reproduktion auf das Failover-Ziel kopiert werden, sodass sie beim Start der VM vom Konfigurationsdienst installiert werden können. Dieser Vorgang wird automatisch ausgeführt, wenn das Failover-Ziel eine Verbindung zum Protect-Server herstellen kann. Wird der Vorgang nicht ausgeführt, müssen Sie die Umgebung vor der Reproduktion anhand der folgenden Schritte vorbereiten:

1 Rufen Sie die VMware Tools-Pakete von einem ESX-Host ab:

1a Kopieren Sie mit `scp` das Image `windows.iso` aus dem Verzeichnis `/usr/lib/vmware/isoimages` auf einem zugänglichen VMware-Host in einen lokalen temporären Ordner.

1b Öffnen Sie das ISO-Image, extrahieren Sie die Setup-Pakete und speichern Sie sie an einem verfügbaren Speicherort:

- **VMware 5.0 und 5.1:** Die Setup-Pakete bestehen aus den Dateien `setup.exe` und `setup64.exe`.
- **VMware 4.0 und 4.1:** Die Setup-Pakete bestehen aus den Dateien `VMware Tools.msi` und `VMware Tools64.msi`.

2 Erstellen Sie aus den vom VMware Server extrahierten Setup-Paketen OFX-Pakete:

2a Komprimieren Sie das gewünschte Paket. Stellen Sie dabei sicher, dass sich die Setup-Installationsdatei auf der Root-Ebene des `.zip`-Archivs befindet.

2b Benennen Sie das `.zip`-Archiv in `1.package` um, sodass es als OFX-Paket verwendet werden kann.

HINWEIS: Wenn Sie ein OFX-Paket von mehr als einem Setup-Paket erstellen möchten, beachten Sie, dass für jedes Setup-Paket ein eigenes eindeutiges `.zip`-Archiv erforderlich ist.

Da jedes Paket den gleichen Namen (`1.package`) hat, müssen Sie beim Speichern mehrerer `.zip`-Archive als OFX-Paket für jedes Paket ein eigenes Unterverzeichnis anlegen.

---

3 Kopieren Sie das entsprechende OFX-Paket (`1.package`) in `%ProgramFiles(x86)%\PlateSpin\Packages\%`*`GUID`*`%` auf dem PlateSpin Server. Der Wert `%`*`GUID`*`%` hängt von der Version Ihres VMware Servers und der Architektur der VMware Tools ab.

In der folgenden Tabelle sind die Serverversionen, die VMware Tools-Architektur und der GUID-Bezeichner aufgeführt, die Sie zum Kopieren des Pakets in das richtige Verzeichnis benötigen:

VMware Server Version	VMware Tools-Architektur	GUID
4.0	x86	D052CBAC-0A98-4880-8BCC-FE0608F0930F
4.0	x64	80B50267-B30C-4001-ABDF-EA288D1FD09C
4.1	x86	F2957064-65D7-4bda-A52B-3F5859624602
4.1	x64	80B1C53C-6B43-4843-9D63-E9911E9A15D5
5,0	x86	AD4FDE1D-DE86-4d05-B147-071F4E1D0326
5,0	x64	F7C9BC91-7733-4790-B7AF-62E074B73882
5.1	x86	34DD2CBE-183E-492f-9B36-7A8326080755
5.1	x64	AD4FDE1D-DE86-4d05-B147-071F4E1D0326

Beschleunigen des Konfigurationsprozesses

Nach dem Booten des Failover-Ziels wird der Konfigurationsdienst gestartet, um die Verwendung der VM vorzubereiten. Er bleibt jedoch einige Minuten inaktiv und wartet auf Daten vom PlateSpin Server bzw. sucht auf der CD ROM nach VMware Tools. So verkürzen Sie die Wartezeit:

1. Navigieren Sie auf der Webseite für die Konfiguration zur Konfigurationseinstellung `ConfigurationServiceValues`, und ändern Sie den Wert der untergeordneten Einstellung `WaitForFloppyTimeoutInSecs` in null (0).
2. Navigieren Sie auf der Webseite für die Konfiguration zum Parameter `ForceInstallVMToolsCustomPackage`, und ändern Sie den Wert in `wahr`.

Mit diesen Einstellungen dauert der Konfigurationsprozess weniger als 15 Minuten: der Zielcomputer wird (maximal zweimal) neu gestartet, die VMware Tools werden installiert und SRM greift auf die Tools zu, um das Konfigurieren von Networking am Remotestandort zu unterstützen.

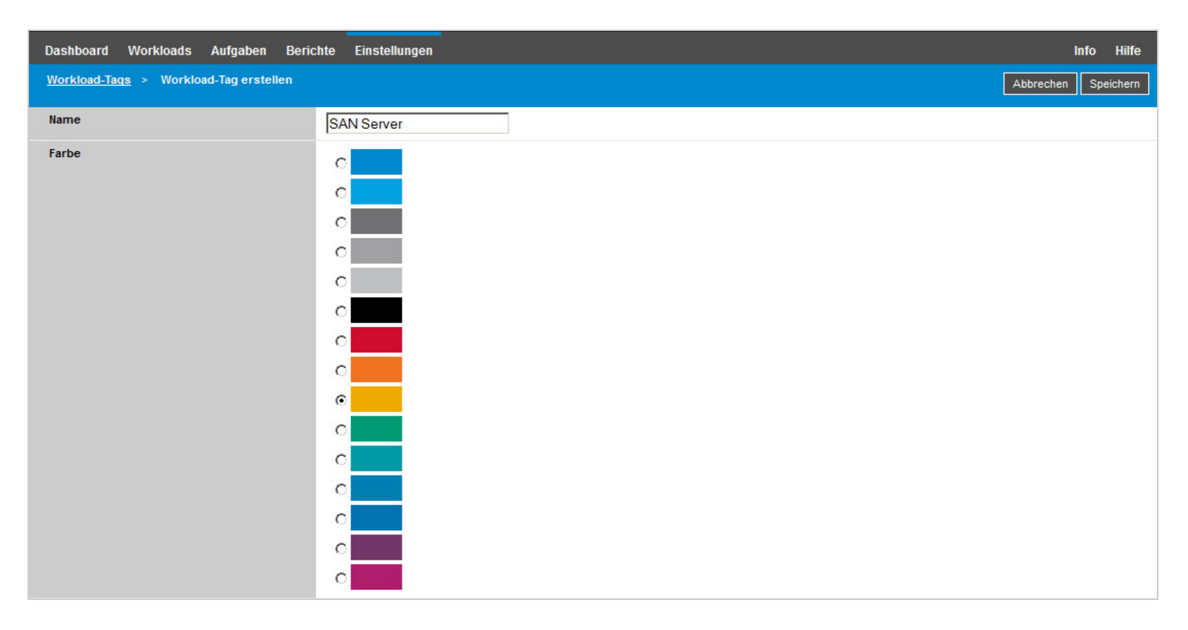
2.4.5 Sortieren von Workloads mithilfe von Tags

Die Workloads-Ansicht in der Protect-Weboberfläche enthält unter Umständen eine sehr lange Liste mit Workloads. Das Durchsuchen dieser Workloads zum Ausführen von Aktionen für ähnliche Workloads kann äußerst zeitaufwendig werden.

Zur einfachen Sortierung der Workload-Liste können Sie einem oder mehreren Workloads in der Workload-Liste optional ID-Tags zuweisen, so dass sie mit einer eindeutigen Farbe und Beschreibung gekennzeichnet werden. Wenn Tags zugeordnet sind, können Sie die Liste nach dem Tag-Attribut sortieren. Hierbei werden die Tags gruppiert, was die Massenauswahl für das Festlegen von Aktionen erleichtert.

So richten Sie Workload-Tags ein:

1. Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen > Workload-Tags > Workload-Tag erstellen**. Die Seite „Workload-Tag erstellen“ wird geöffnet.



Auf dieser Seite können Sie einen Tag-Namen (max. 25 Zeichen) angeben und dieser Beschreibung eine Farbe zuweisen. Sie können beliebig viele eindeutige Tags anlegen; die Auswahl an Farben ist allerdings begrenzt.

Beim Speichern wird das neue Tag auf der Seite „Einstellungen“ in der Ansicht „Workload-Tags“ in die Liste der verfügbaren Workload-Tags aufgenommen. In dieser Ansicht können Sie die Tags in der Liste bearbeiten oder löschen.

Auf der Seite „Workloads“ in der Spalte „Tag“ wird jeweils das eindeutige Tag angezeigt, das Sie den einzelnen Workloads zugewiesen haben. Beim Sortieren nach dieser Spalte können Sie die Tags gruppieren und so verfügbare Aktionen gleichzeitig für diese getaggten Workloads ausführen.

So weisen Sie ein einzelnes Tag einem Workload zu:

1. Wählen Sie in der Liste der Workloads den zu taggenden Workload aus, und klicken Sie auf **Konfigurieren**. Die Konfigurationsseite für diesen Workload wird geöffnet.
2. Öffnen Sie auf der Konfigurationsseite unter „Tag“ die Dropdown-Liste, wählen Sie den Namen des Tags aus, das dem Workload zugewiesen werden soll, und klicken Sie auf **Speichern**.

Weitere Informationen zu Tags

Beachten Sie auch die folgenden Informationen zu Workload-Tags:

- Wenn Sie einen Workload auf einen neuen Server exportieren, bleiben seine Tag-Einstellungen erhalten.
- Sie können ein Tag nicht löschen, wenn es noch mindestens einem Workload in der Liste zugewiesen ist.
- Soll ein Tag aus einem Workload entfernt werden (also seine Zuweisung aufgehoben werden), wählen Sie in der Dropdown-Liste der Tag-Namen den „leeren“ Eintrag aus.

3 Aufgestellt und in Betrieb

In diesem Kapitel werden die wichtigsten Funktionen von PlateSpin Protect und seiner Schnittstelle beschrieben.

3.1 Starten der PlateSpin Protect-Weboberfläche

Die meisten Aktionen mit der Appliance führen Sie über den browserbasierten PlateSpin Protect-Web-Client durch.

Die folgenden Browser werden unterstützt:

- *Google Chrome*, Version 34.0 und höher
- *Microsoft Internet Explorer*, Version 11.0 und höher
- *Mozilla Firefox*, Version 29.0 und höher

HINWEIS: JavaScript (Active Scripting) muss in Ihrem Browser aktiviert sein:

- **Chrome:** Wählen Sie im Chrome-Menü **Einstellungen**, blättern Sie zu **Erweiterte Einstellungen anzeigen** und wählen Sie diese Option aus. Wählen Sie dann **Inhaltseinstellungen** > **Ausführung von JavaScript für alle Websites zulassen** aus.
- **IE:** Wählen Sie im Menü „Extras“ den Eintrag **Internetoptionen** > **Sicherheit**. Klicken Sie auf **Stufe Anpassen**. Blättern Sie zu **Active Scripting**, und wählen Sie diesen Eintrag aus. Wählen Sie **Aktivieren**, klicken Sie im Warnfenster auf **Ja**, und klicken Sie auf **OK** und dann auf **Anwenden** > **OK**.
- **Firefox:** Klicken Sie auf **Extras** > **Einstellungen** > **Inhalt** und wählen Sie anschließend die Option **JavaScript aktivieren** aus.

Informationen zur Verwendung der PlateSpin Protect-Weboberfläche und der integrierten Hilfe in einer der unterstützten Sprachen finden Sie unter Abschnitt 2.4.2, „Einrichtung der Sprache bei internationalen Versionen von PlateSpin Protect“, auf Seite 38.

So starten Sie die PlateSpin Protect-Weboberfläche:

1 Öffnen Sie einen Webbrowser und wechseln Sie zu folgender Adresse:

   `http://`*<Hostname | IP-Adresse>*`/Protect`

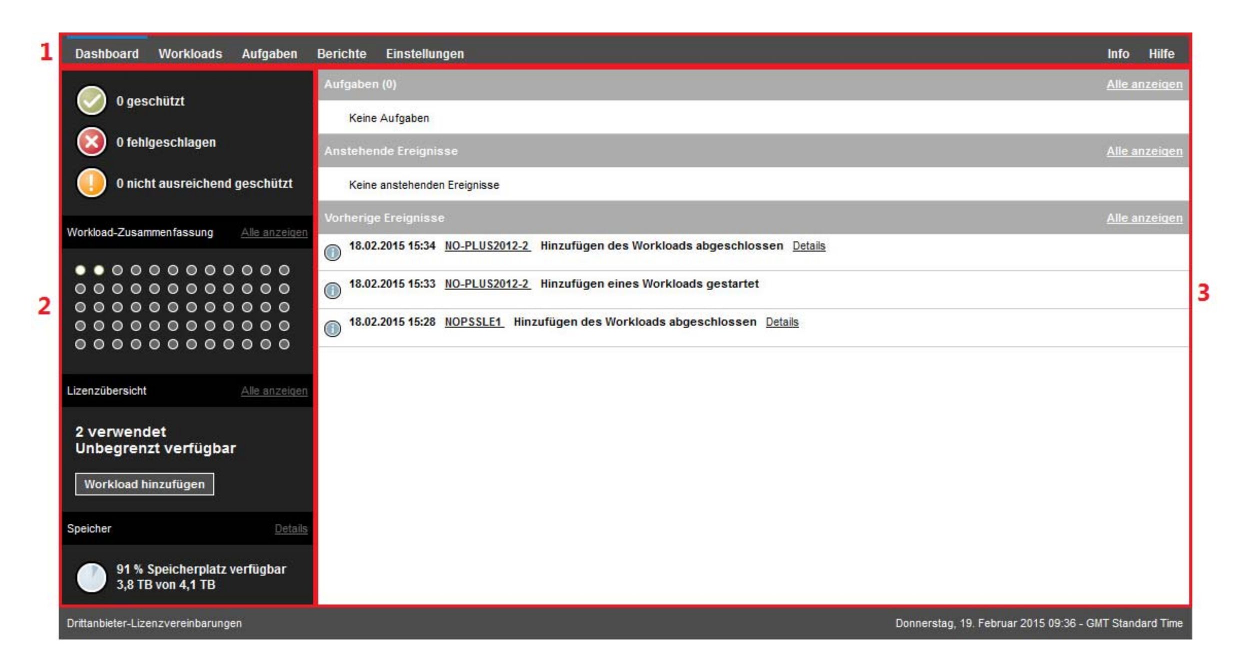
   Ersetzen Sie *<Hostname | IP-Adresse>* durch den Hostnamen oder die IP-Adresse Ihres PlateSpin Server-Hosts.

   Wenn SSL nicht aktiviert ist, verwenden Sie `http` in der URL.

3.2 Elemente der PlateSpin Protect-Weboberfläche

Die Standardoberfläche der PlateSpin Protect-Weboberfläche ist die Seite „Dashboard", die Elemente zum Navigieren zu verschiedenen Funktionsbereichen der Oberfläche und zum Durchführen von Workload-Schutz- und Wiederherstellungsaufgaben bereitstellt.

***Abbildung 3-1** Die Standard-Dashboard-Seite der PlateSpin Protect-Weboberfläche*



Die Dashboard-Seite besteht aus den folgenden Elementen:

1. **Navigationsleiste:** Auf den meisten Seiten der PlateSpin Protect-Weboberfläche enthalten.
2. **Teilfenster mit visueller Zusammenfassung:** Bietet einen umfassenden Überblick über den Gesamtstatus des Workload-Inventars von PlateSpin Protect.
3. **Teilfenster mit Aufgaben und Ereignissen:** Bietet Informationen über Ereignisse und Aufgaben, die einen Eingriff des Benutzers erfordern.

Die folgenden Abschnitte enthalten weitere Informationen.

- Abschnitt 3.2.1, „Navigationsleiste", auf Seite 49
- Abschnitt 3.2.2, „Teilfenster mit visueller Zusammenfassung", auf Seite 49
- Abschnitt 3.2.3, „Teilfenster mit Aufgaben und Ereignissen", auf Seite 50

HINWEIS: Sie können bestimmte Elemente der Weboberfläche an das Markenbild Ihres Unternehmens anpassen. Weitere Informationen finden Sie in Anhang C, „Anpassen der PlateSpin Protect-Weboberfläche an das Markenbild", auf Seite 129.

3.2.1 Navigationsleiste

Die Navigationsleiste enthält folgende Links:

- **Dashboard:** Zeigt die Standardseite „Dashboard“ an.
- **Workloads:** Zeigt die Seite „Workloads“ an. Weitere Informationen hierzu finden Sie unter „Workloads und Workload-Befehle“, auf Seite 50.
- **Aufgaben:** Zeigt die Seite „Aufgaben“ mit den Elementen an, die einen Benutzereingriff erfordern.
- **Berichte:** Zeigt die Seite „Berichte“ an. Weitere Informationen hierzu finden Sie unter „Generieren von Workload- und Workload-Schutz-Berichten“, auf Seite 55.
- **Einstellungen:** Zeigt die Seite „Einstellungen“ an, die Zugriff auf die folgenden Konfigurationsoptionen bietet:
  - **Schutzebenen:** Weitere Informationen hierzu finden Sie unter „Schutzebenen“, auf Seite 84.
  - **Workload Tags:** Weitere Informationen hierzu finden Sie unter „Sortieren von Workloads mithilfe von Tags“, auf Seite 44.
  - **Berechtigungen:** Weitere Informationen hierzu finden Sie in „Einrichten der Benutzerautorisierung und -authentifizierung“, auf Seite 25.
  - **Container:** Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern (Schutzziele)“, auf Seite 59.
  - **Benachrichtigungseinstellungen:** „Einrichten automatischer Ereignisbenachrichtigungen per Email“, auf Seite 35.
  - **Einstellungen für Reproduktionsberichte:** „Einrichten automatischer Reproduktionsberichte per Email“, auf Seite 37
  - **SMTP:** Weitere Informationen hierzu finden Sie unter „SMTP-Konfiguration“, auf Seite 35.
  - **Lizenzen:** Weitere Informationen hierzu finden Sie in „Produktlizenzierung“, auf Seite 23.

3.2.2 Teilfenster mit visueller Zusammenfassung

Im Fenster „Visuelle Zusammenfassung“ werden effizient alle lizenzierten Workloads sowie die Menge an verfügbarem Speicher angezeigt.

Inventarisierte Workloads werden in drei Kategorien dargestellt:

- **Geschützt:** Gibt die Anzahl der aktiv geschützten Workloads an.
- **Fehlgeschlagen:** Gibt die Anzahl der geschützten Workloads an, die das System gemäß der Schutzebene dieses Workloads als fehlgeschlagen ausgegeben hat.
- **Nicht ausreichend geschützt:** Gibt die Anzahl der geschützten Workloads an, die einen Eingriff des Benutzers erfordern.

Der Bereich in der Mitte des linken Teilfensters stellt eine grafische Zusammenfassung der Seite „Workloads“ dar. Er verwendet Punktsymbole, um die verschiedenen Statusformen der Workloads anzuzeigen:

***Tabelle 3-1** Punktsymbol-Darstellung des Workload-Status*

● Ungeschützt	● **Nicht ausreichend geschützt**
○ **Ungeschützt – Fehler**	● **Fehlgeschlagen**

Geschützt	Abgelaufen
Nicht verwendet	

Die Symbole werden in alphabetischer Reihenfolge gemäß dem Workload-Namen angezeigt. Richten Sie den Mauszeiger auf ein Punktsymbol, um den Namen des Workloads anzuzeigen, oder klicken Sie darauf, um die zugehörige Seite mit den Workload-Details zu öffnen.

Speicher bietet Informationen über den für PlateSpin Protect verfügbaren Container-Speicherplatz.

3.2.3 Teilfenster mit Aufgaben und Ereignissen

Das Teilfenster mit den Aufgaben und Ereignissen zeigt die letzten Aufgaben und vorherigen Ereignisse sowie die nächsten anstehenden Ereignisse an.

Ereignisse werden protokolliert, wenn sie für das System oder den Workload relevant sind. Ereignisse sind beispielsweise das Hinzufügen eines neuen geschützten Workloads, das Starten oder Fehlschlagen der Reproduktion eines Workloads oder die Erkennung eines Fehlers eines geschützten Workloads. Einige Ereignisse generieren automatische Email-Benachrichtigungen, wenn SMTP konfiguriert ist. Weitere Informationen hierzu finden Sie in „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“, auf Seite 35.

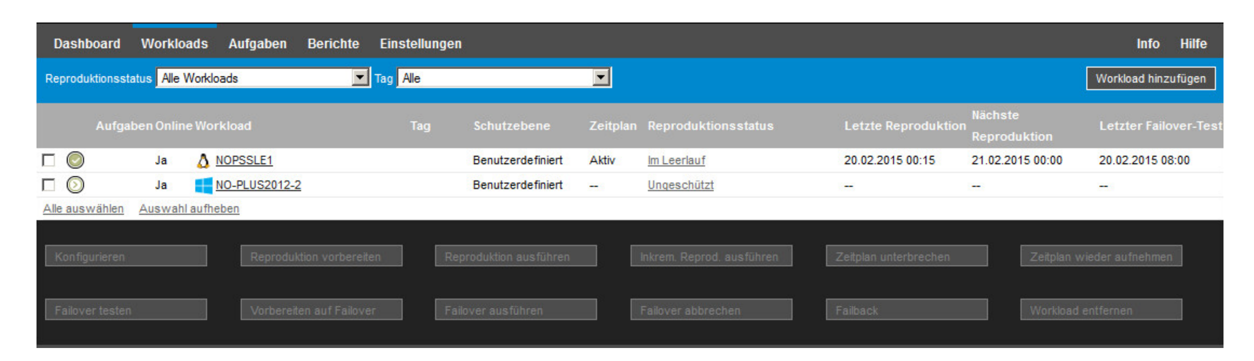
Aufgaben sind spezielle Befehle, die mit Ereignissen verbunden sind, die den Eingriff des Benutzers erfordern. Beispiel: Nach Abschluss des Befehls „Failover testen“ generiert das System ein Ereignis, das mit zwei Aufgaben verbunden ist: `Mark. 'Test erfolgr.'` und `Mark. 'Test n. best.'`. Wenn Sie auf eine der Aufgaben klicken, wird der Failover-Test abgebrochen und es wird ein entsprechendes Ereignis in das Protokoll geschrieben. Ein weiteres Beispiel ist das Ereignis `FullReplicationFailed`, das zusammen mit einer `StartFull`-Aufgabe gezeigt wird. Sie finden eine vollständige Liste der aktuellen Aufgaben auf der Registerkarte **Aufgaben**.

Im Teilfenster „Aufgaben und Ereignisse“ auf dem Dashboard werden für jede Kategorie maximal drei Einträge angezeigt. Wenn alle Aufgaben oder vergangene und anstehende Ereignisse angezeigt werden sollen, klicken Sie im entsprechenden Abschnitt auf **Alle anzeigen**.

3.3 Workloads und Workload-Befehle

Die Seite „Workloads“ enthält eine Tabelle mit einer Zeile pro inventarisiertem Workload. Klicken Sie auf einen Workload-Namen, um die zugehörige Seite „Workload-Details“ anzuzeigen, in der Sie für den Workload und seinen Status relevante Konfigurationen ansehen und bearbeiten können.

***Abbildung 3-2** Die Seite „Workloads“*

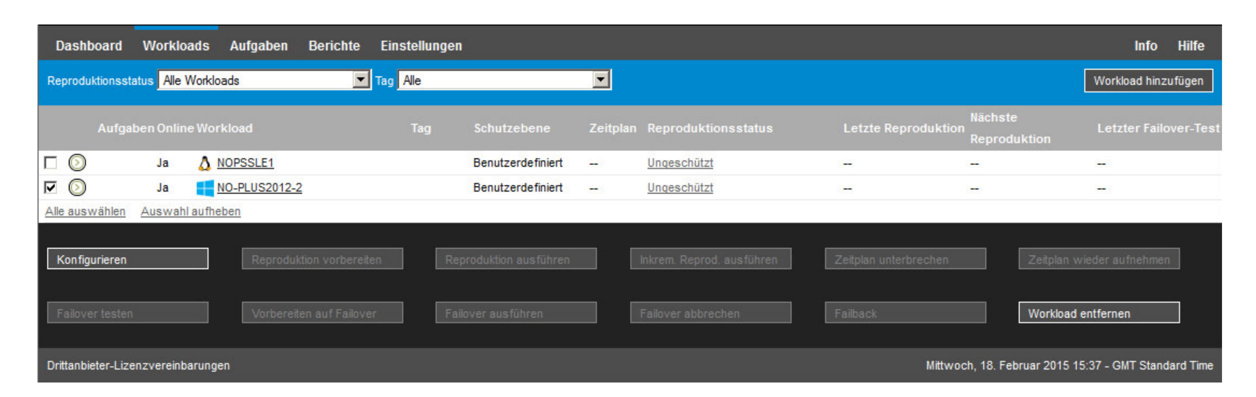


HINWEIS: Alle Zeitstempel entsprechen der Zeitzone des PlateSpin Server-Hosts. Diese kann sich von der Zeitzone des geschützten Workloads oder der Zeitzone des Hosts, auf dem Sie die PlateSpin Protect-Weboberfläche ausführen, unterscheiden. Unten rechts im Client-Fenster werden das Serverdatum und die Serveruhrzeit angezeigt.

3.3.1 Workload-Schutz- und Wiederherstellungsbefehle

Befehle spiegeln den Workflow des Workload-Schutzes und der Wiederherstellung wider. Wählen Sie zur Ausführung eines Befehls für einen Workload das entsprechende Kontrollkästchen auf der linken Seite aus. Anwendbare Befehle hängen vom aktuellen Status eines Workloads ab.

***Abbildung 3-3** Workload-Befehle*



In der folgenden Tabelle finden Sie eine Übersicht über die Workload-Befehle sowie deren Beschreibung.

***Tabelle 3-2** Workload-Schutz- und Wiederherstellungsbefehle*

Workload-Befehl	Beschreibung
Konfigurieren	Startet die Konfiguration des Workload-Schutzes mit Parametern, die auf einen inventarisierten Workload anwendbar sind.
Reproduktion vorbereiten	Installiert die erforderliche Datentransfersoftware im Quell-Container und erstellt einen Failover-Workload (einen virtuellen Computer) im Ziel-Container zur Vorbereitung der Workload-Reproduktion.
Reproduktion ausführen	Startet die Reproduktion des Workloads entsprechend der angegebenen Parameter (vollständige Reproduktion).
Inkrementell ausführen	Führt eine inkrementelle Übertragung von geänderten Daten vom Ursprung zum Ziel außerhalb der im Vertrag für den Workload-Schutz festgelegten Zeiten durch.
Zeitplan unterbrechen	Setzt den Schutz aus; alle geplanten Reproduktionen werden übersprungen bis der Zeitplan wieder aufgenommen wird.
Zeitplan wieder aufnehmen	Nimmt den Schutz gemäß den gespeicherten Schutzeinstellungen wieder auf.
Failover testen	Bootet und konfiguriert den Failover-Workload für Testzwecke in einer isolierten Umgebung innerhalb des Containers.
Vorbereiten auf Failover	Bootet den Failover-Workload in Vorbereitung eines Failover-Vorgangs.

Workload-Befehl	Beschreibung
Failover ausführen	Bootet und konfiguriert den Failover-Workload, der die Geschäftsdienste eines fehlgeschlagenen Workloads übernimmt.
Failover abbrechen	Bricht den Failover-Vorgang ab.
Failback	Überführt den Failover-Workload nach einem Failover-Vorgang per Failback wieder in die ursprüngliche oder in eine neue Infrastruktur (virtuell oder physisch).
Workload entfernen	Entfernt einen Workload aus dem Inventar.

3.4 Verwalten mehrerer Instanzen von PlateSpin Protect und PlateSpin Forge

PlateSpin Protect enthält eine webbasierte Client-Anwendung, die PlateSpin Protect-Verwaltungskonsole, die zentralen Zugriff auf mehrere Instanzen von PlateSpin Protect und PlateSpin Forge bietet.

In einem Rechenzentrum mit mehreren Instanzen von PlateSpin Protect können Sie eine der Instanzen als Manager festlegen und die Verwaltungskonsole von dort aus ausführen. Weitere Instanzen werden unter dem Manager hinzugefügt, sodass ein zentraler Punkt für die Steuerung und Interaktion zur Verfügung steht.

- Abschnitt 3.4.1, „Verwenden der PlateSpin Protect-Verwaltungskonsole“, auf Seite 52
- Abschnitt 3.4.2, „Informationen zu PlateSpin Protect-Verwaltungskonsolenkarten“, auf Seite 53
- Abschnitt 3.4.3, „Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole“, auf Seite 54
- Abschnitt 3.4.4, „Verwalten von Karten auf der Verwaltungskonsole“, auf Seite 54

3.4.1 Verwenden der PlateSpin Protect-Verwaltungskonsole

1. Öffnen Sie einen Webbrowser auf einem Computer, der Zugriff auf die PlateSpin Protect-Instanzen hat, und navigieren Sie zu folgender URL:

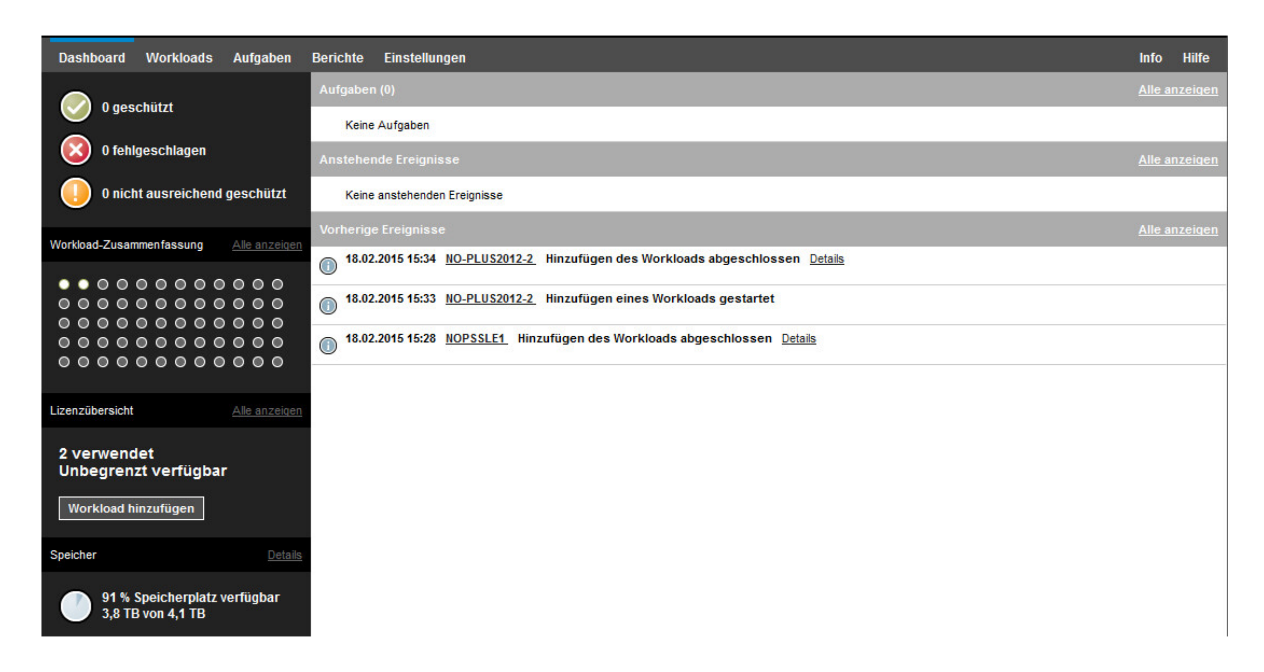
   `https://`*<IP-Adresse* | *Hostname>*`/console`.

   Ersetzen Sie *<IP-Adresse* | *Hostname>* durch die IP-Adresse oder den Hostnamen des PlateSpin Server-Hosts, der als Manager festgelegt wurde.

2. Melden Sie sich mit Ihrem Benutzernamen und Passwort an.

   Die Standardseite „Dashboard“ der Konsole wird angezeigt.

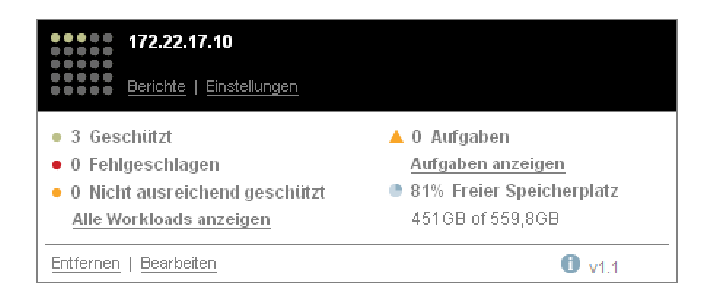
Abbildung 3-4 Die Standardseite „Dashboard“ der Verwaltungskonsole



3.4.2 Informationen zu PlateSpin Protect-Verwaltungskonsolenkarten

Einzelne Instanzen von PlateSpin Protect und PlateSpin Forge werden nach dem Hinzufügen zur Verwaltungskonsole als Karten dargestellt.

Abbildung 3-5 PlateSpin Protect-Instanzkarte



Eine Karte zeigt grundlegende Informationen über die spezifische Instanz von PlateSpin Protect oder PlateSpin Forge an, z. B.:

- IP-Adresse/Hostname
- Standort
- Versionsnummer
- Workload-Anzahl
- Workload-Status
- Speicherkapazität
- Verbleibender freier Speicherplatz

Hyperlinks auf jeder Karte ermöglichen Ihnen die Navigation zu den für diese Instanz spezifischen Seiten „Workloads“, „Berichte“, „Einstellungen“ und „Aufgaben“. Es gibt darüber hinaus Hyperlinks, über die Sie die Konfiguration einer Karte bearbeiten oder eine Karte aus der Anzeige entfernen können.

3.4.3 Hinzufügen von Instanzen von PlateSpin Protect und PlateSpin Forge zur Verwaltungskonsole

Beim Hinzufügen einer PlateSpin Protect oder Forge-Instanz zur Verwaltungskonsole wird eine neue Karte zum Dashboard der Verwaltungskonsole hinzugefügt.

HINWEIS: Wenn Sie sich bei einer Verwaltungskonsole anmelden, die auf einer Instanz von PlateSpin Protect oder PlateSpin Forge ausgeführt wird, wird diese Instanz der Konsole nicht automatisch hinzugefügt. Sie muss manuell hinzugefügt werden.

So fügen Sie eine PlateSpin Protect oder Forge-Instanz zur Konsole hinzu:

1. Klicken Sie im Haupt-Dashboard der Konsole auf **PlateSpin-Server hinzufügen**.

   Die Seite **Hinzufügen/Bearbeiten** wird angezeigt.
2. Geben Sie die URL des PlateSpin-Server-Hosts oder des virtuellen Computers mit PlateSpin Forge an. Verwenden Sie HTTPS, wenn SSL aktiviert ist.
3. (Optional) Aktivieren Sie das Kontrollkästchen **Berechtigungsnachweis der Verwaltungskonsole verwenden**, um denselben Berechtigungsnachweis zu verwenden, der von der Konsole verwendet wird. Wenn diese Option ausgewählt ist, füllt die Konsole automatisch das Feld **Domäne\Benutzername** aus.
4. Geben Sie im Feld **Domäne\Benutzername** einen Domänennamen und einen Benutzernamen ein, die für die von Ihnen hinzugefügte PlateSpin Protect- oder Plate Spin Forge-Instanz gültig sind. Geben Sie im Feld **Passwort** das entsprechende Passwort ein.
5. (Optional) Geben Sie einen beschreibenden oder identifizierenden **Anzeigenamen** (max. 15 Zeichen), einen **Speicherort** (max. 20 Zeichen) und ggf. erforderliche **Hinweise** ein (max. 400 Zeichen).
6. Klicken Sie auf **Hinzufügen/Speichern**.

   Es wird eine neue Karte zum Dashboard hinzugefügt.

3.4.4 Verwalten von Karten auf der Verwaltungskonsole

Sie können die Details einer Karte auf der Verwaltungskonsole ändern.

1. Klicken Sie auf den Hyperlink **Bearbeiten** auf der Karte, die Sie bearbeiten möchten.

   Die Seite **Hinzufügen/Bearbeiten** der Konsole wird angezeigt.
2. Nehmen Sie alle gewünschten Änderungen vor und klicken Sie anschließend auf **Hinzufügen/ Speichern**.

   Das aktualisierte Konsolen-Dashboard wird angezeigt.

So entfernen Sie eine Karte von der Verwaltungskonsole:

1. Klicken Sie auf den Hyperlink **Entfernen** auf der Karte, die Sie entfernen möchten.

   Es wird eine Bestätigungsaufforderung angezeigt.

2 Klicken Sie auf **OK**.

Die individuelle Karte wird vom Dashboard entfernt.

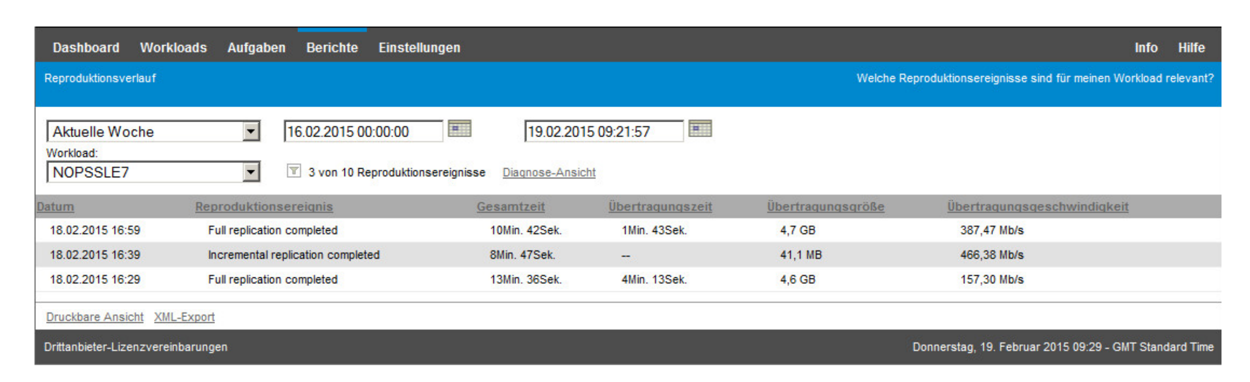
3.5 Generieren von Workload- und Workload-Schutz-Berichten

PlateSpin Protect ermöglicht Ihnen das Generieren von Berichten, die einen analytischen Einblick in Ihre Workload-Schutzverträge über einen bestimmten Zeitraum hinweg gewähren.

Die folgenden Berichtstypen werden unterstützt:

- **Workload-Schutz:** Bericht über Reproduktionsereignisse für alle Workloads in einem auswählbaren Zeitraum.
- **Reproduktionsverlauf:** Bericht über Reproduktionstyp, Größe, Zeit und Übertragungsgeschwindigkeit pro auswählbarem Workload in einem auswählbaren Zeitraum.
- **Reproduktionsfenster:** Bericht über die Dynamik vollständiger und inkrementeller Reproduktionen, die nach **Durchschnitt**, **Zuletzt**, **Summe** und **Spitze** zusammengefasst werden können.
- **Aktueller Schutzstatus:** Statistikbericht über die Parameter **Ziel-RPO**, **RPO (tatsächlich)**, **TTO (tatsächlich)**, **RTO (tatsächlich)**, **Letzter Failover-Test**, **Letzte Reproduktion** und **Testalter**.
- **Ereignisse:** Bericht über Systemereignisse für alle Workloads in einem auswählbaren Zeitraum.
- **Routineereignisse:** Bericht über anstehende Workload-Schutz-Ereignisse.

***Abbildung 3-6** Optionen für einen Reproduktionsverlaufsbericht*



So erzeugen Sie einen Bericht:

1 Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Berichte**.

Es wird eine Liste mit Berichtstypen angezeigt.

2 Klicken Sie auf den Namen des erforderlichen Berichtstyps.

4 Workload-Schutz

PlateSpin Protect erstellt eine Reproduktion Ihres Produktions-Workloads und aktualisiert diese Reproduktion auf Basis eines von Ihnen festgelegten Zeitplans.

Die Reproduktion bzw. der *Failover-Workload* ist eine virtuelle Maschine im VM-Container von PlateSpin Protect und übernimmt die Geschäftsfunktion des Produktions-Workloads, falls es zu einer Störung am Produktionsstandort kommt.

4.1 Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung

PlateSpin Protect definiert folgenden Workflow für den Workload-Schutz und die Wiederherstellung:

1 **Vorbereitung:** Für diesen Schritt fallen Vorbereitungsschritte an, mit denen sichergestellt werden soll, dass Ihre Workloads, die Container und die Umgebung die erforderlichen Kriterien erfüllen.

   1a Stellen Sie sicher, dass PlateSpin Protect Ihren Workload unterstützt.

   Weitere Informationen hierzu finden Sie unter „Unterstützte Konfigurationen“, auf Seite 13.

   1b Stellen Sie sicher, dass Ihre Workloads und Container die Zugriffs- und Netzwerkvoraussetzungen erfüllen.

   Weitere Informationen hierzu finden Sie in „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 29.

   1c (nur Linux)

   - (Bedingt) Wenn Sie planen, einen unterstützten Linux-Workload zu schützen, der einen nicht-standardmäßigen, benutzerdefinierten oder neueren Kernel hat, bauen Sie das PlateSpin `blkwatch`-Modul neu auf, das für eine Datenreproduktion auf Blockebene erforderlich ist.

     Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7005873.
   - (Empfohlen) Bereiten Sie LVM-Snapshots für den Datentransfer auf Blockebene vor. Stellen Sie sicher, dass jede Volume-Gruppe über genügend freien Speicherplatz für LVM-Snapshots verfügt (mindestens 10 % der Summe aller Partitionen).

Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7005872.

- (Optional) Bereiten Sie die Skripte `freeze` und `thaw` vor, so dass sie bei jeder Reproduktion auf dem Ursprungs-Workload ausgeführt werden.

  Weitere Informationen hierzu finden Sie unter „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)“, auf Seite 88.

2. **Inventar:** In diesem Schritt fügen Sie Workloads und Container in die PlateSpin-Server-Datenbank ein.

   Workloads, die Sie schützen möchten, sowie Container, auf denen Failover-Workloads gehostet werden, müssen ordnungsgemäß inventarisiert werden. Sie können Workloads und Container jedem beliebigen Ordner hinzufügen, doch jeder Schutzvertrag erfordert einen definierten Workload und Container, der vom PlateSpin-Server inventarisiert wurde. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern (Schutzziele)“, auf Seite 59 und „Hinzufügen von Workloads für den Schutz“, auf Seite 60.

3. **Definition des Schutzvertrags:** In diesem Schritt definieren Sie die Details und die Spezifikationen des Schutzvertrags, und Sie bereiten die Reproduktion vor.

   Weitere Informationen hierzu finden Sie unter „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“, auf Seite 61.

4. **Initiieren des Schutzes:** Mit diesem Schritt beginnt der Schutzvertrag gemäß Ihren Anforderungen.

   Weitere Informationen hierzu finden Sie unter „Starten des Workload-Schutzes“, auf Seite 65.

5. **Optionale Schritte im Schutz-Lebenszyklus:** Diese Schritte gehören nicht zum automatisierten Reproduktionsplan, sind jedoch in verschiedenen Situationen von Nutzen oder auch aufgrund Ihrer Strategie zur Aufrechterhaltung des ununterbrochenen Geschäftsbetriebs unerlässlich.

   - *Manuell/inkrementell*. Mit **Inkrementelle Reproduktion ausführen** starten Sie manuell eine inkrementelle Reproduktion außerhalb des Workload-Schutzvertrags.
   - *Testbetrieb*. Die Failover-Funktion lässt sich auf kontrollierte Weise in einer kontrollierten Umgebung testen. Weitere Informationen hierzu finden Sie unter Verwenden der Funktion „Failover testen“.

6. **Failover:** Mit diesem Schritt wird ein Failover des geschützten Workloads auf die Reproduktion vorgenommen, die in Ihrem VM-Container ausgeführt wird. Weitere Informationen hierzu finden Sie unter „Failover“, auf Seite 66.

7. **Failback:** Dieser Schritt entspricht der Phase der Wiederaufnahme des Betriebs, nachdem Sie die Probleme mit dem Produktions-Workload behoben haben. Weitere Informationen hierzu finden Sie unter „Failback“, auf Seite 68.

8. **Erneuter Schutz:** In diesem Schritt definieren Sie den ursprünglichen Schutzvertrag für den Workload neu. Weitere Informationen hierzu finden Sie in „Erneutes Schützen eines Workloads“, auf Seite 73

Der Großteil dieser Schritte kann über Workload-Befehle auf der Seite „Workloads“ durchgeführt werden. Weitere Informationen hierzu finden Sie unter „Workloads und Workload-Befehle“, auf Seite 50.

Der Befehl **Erneut schützen** steht nach einem erfolgreichen Failback-Vorgang zur Verfügung.

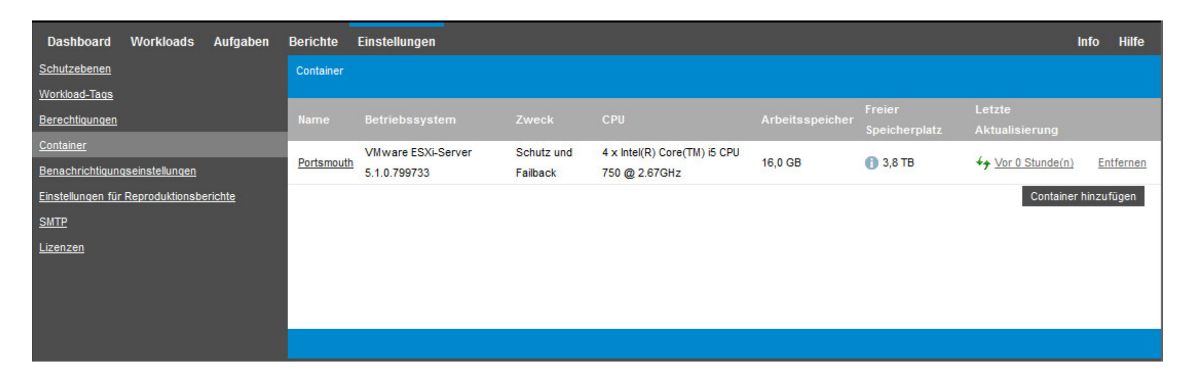
4.2 Hinzufügen von Containern (Schutzziele)

Ein Container ist eine Schutz-Infrastruktur, die als Host für die regelmäßig aktualisierte Reproduktion eines geschützten Workloads agiert. Diese Infrastruktur kann entweder ein VMware ESX-Server oder ein VMware DRS-Cluster sein.

Um einen Workload schützen zu können, benötigen Sie einen Workload und Container, der vom PlateSpin-Server inventarisiert (oder diesem Server *hinzugefügt*) ist.

So fügen Sie einen Container hinzu:

1 Klicken Sie auf der PlateSpin Protect-Weboberfläche auf **Einstellungen > Container > Container hinzufügen**.



2 Geben Sie die folgenden Parameter an:

- **Typ:** Wählen Sie den Containertyp aus (**VMware ESX-Server** oder **VMware DRS-Cluster**). Stellen Sie sicher, dass der Container unterstützt wird.

  Weitere Informationen finden Sie unter „Unterstützte VM-Container“, auf Seite 17.
- **Hostname oder IP-Adresse:** Geben Sie den Hostnamen oder die IP-Adresse des Containers ein.
- **vCenter-Hostname oder -IP-Adresse:** (Nur DRS-Cluster) Geben Sie den Hostnamen oder die IP-Adresse des vCenter-Servers ein.
- **Clustername:** (Nur DRS-Cluster) Geben Sie den Namen des erforderlichen DRS-Clusters ein.

  Wenn Sie versuchen, einen DRS-Cluster hinzuzufügen oder zu aktualisieren, kann der zugrunde liegende Ermittlungsvorgang in folgenden Fällen fehlschlagen:
  - Ein Cluster enthält keine ESX-Hosts.
  - Ein Clustername im vCenter-Server ist nicht eindeutig (auch wenn er einen eindeutigen Inventarpfad hat).
  - Keines der Cluster-Mitglieder ist zugänglich (z. B. weil der vCenter-Server im Wartungsmodus ist).
- **Benutzername/Passwort:** Geben Sie den Administrator-Berechtigungsnachweis für den Zugriff auf den erforderlichen Host ein. Weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 76.
- **Beschreibung:** (Betrifft nur VM-Container) Wählen Sie das erforderliche Element aus (**Schutz, Failback/Bereitstellung** oder beide). Wenn Sie beide Elemente auswählen (**Schutz** und **Failback/Bereitstellung**), steht dieser Container für die Auswahl als Ziel sowohl für Schutz- als auch für Failback-/Bereitstellungsvorgänge zur Verfügung.

3 Klicken Sie auf **Hinzufügen**.

PlateSpin Protect lädt die Seite „Container“ neu und blendet eine Fortschrittsanzeige ( ) für den Container ein, der hinzugefügt wird. Nach Abschluss des Vorgangs ändert sich das Symbol für die Fortschrittsanzeige in das Symbol für **Aktualisieren** .

Klicken Sie zum Aktualisieren eines Containers auf das Symbol **Aktualisieren** neben dem zu aktualisierenden Container. Dadurch wird der Container neu inventarisiert.

Klicken Sie zum Entfernen eines Containers auf **Entfernen** neben dem zu entfernenden Container.

4.3 Hinzufügen von Workloads für den Schutz

Ein Workload, das grundlegende Schutzobjekt in einem Datenspeicher, umfasst ein Betriebssystem, die zugehörige Middleware und die zugehörigen Daten, ist also getrennt von der zugrunde liegenden physischen oder virtuellen Infrastruktur.

Zum Schutz eines Workloads benötigen Sie einen Workload und einen Container, der auf dem PlateSpin-Server inventarisiert (oder diesem Server *hinzugefügt*) ist.

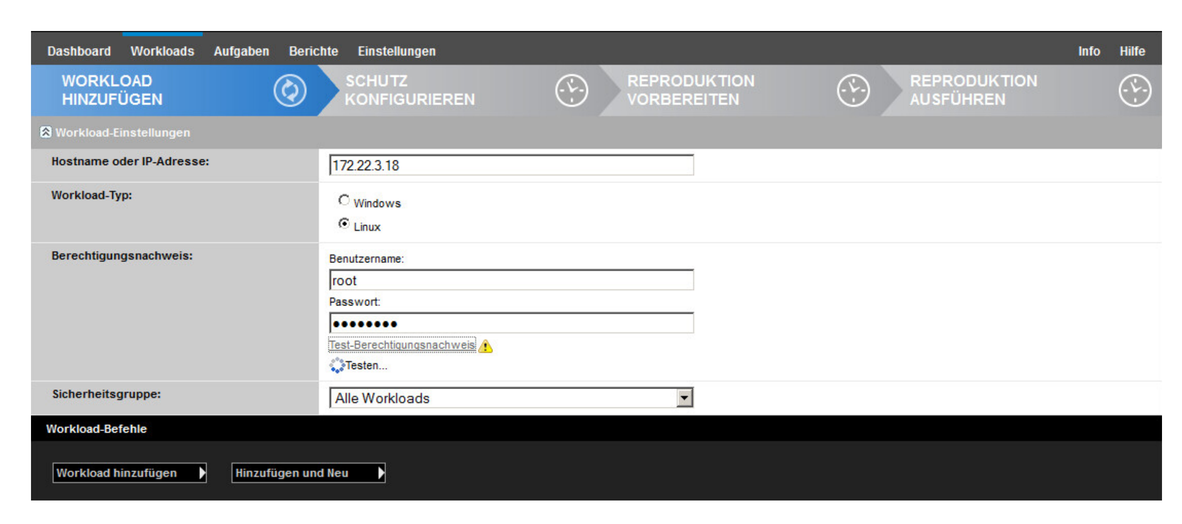
So fügen Sie einen Workload hinzu:

1 Führen Sie die erforderlichen Vorbereitungsschritte durch.

Siehe Schritt 1 unter „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“, auf Seite 57.

2 Klicken Sie auf der Seite „Dashboard“ oder „Workloads“ auf **Workload hinzufügen**.

Auf der PlateSpin Protect-Weboberfläche wird die Seite „Workload hinzufügen“ angezeigt.



3 Geben Sie die erforderlichen Workload-Details an:

- **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Workloads, das Betriebssystem und den Administrator-Berechtigungsnachweis an.

  Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 76).

  Überprüfen Sie, ob **PlateSpin Protect** auf den Workload zugreifen kann. Klicken Sie hierzu auf Test-Berechtigungsnachweis.

4 Klicken Sie auf **Workload hinzufügen**.

   PlateSpin Protect lädt die Seite „Workloads“ neu und blendet eine Fortschrittsanzeige ( ) für den Workload ein, der hinzugefügt wird. Warten Sie, bis der Vorgang abgeschlossen ist. Im Dashboard wird das Ereignis **Workload hinzugefügt** angezeigt, und der neue Workload ist auf der Workload-Seite verfügbar.

Falls Sie noch keinen Container hinzugefügt haben, fügen Sie jetzt einen Container zum Schützen des Workloads hinzu; ansonsten weiter mit „Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion“, auf Seite 61

4.4 Konfigurieren der Schutzdetails und Vorbereiten der Reproduktion

Schutzdetails steuern die Workload-Schutz- und Wiederherstellungseinstellungen sowie das Verhalten im gesamten Lebenszyklus eines geschützten Workloads. In jeder Phase des Schutz- und Wiederherstellungs-Workflows (siehe „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“, auf Seite 57) werden relevante Einstellungen aus den Schutzdetails gelesen.

So konfigurieren Sie die Schutzdetails Ihres Workloads:

1. Fügen Sie einen Workload hinzu. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Workloads für den Schutz“, auf Seite 60.
2. Fügen Sie einen Container hinzu. Weitere Informationen hierzu finden Sie unter „Hinzufügen von Containern (Schutzziele)“, auf Seite 59.
3. Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus und klicken Sie auf **Konfigurieren**.

   Alternativ klicken Sie auf den Namen des Workloads.

   HINWEIS: Wenn das PlateSpin Protect-Inventar noch keinen Container enthält, werden Sie vom System aufgefordert, einen Container hinzuzufügen. Klicken Sie dazu unten auf **Container hinzufügen**.

   ---

4. Wählen Sie eine **Anfängliche Reproduktionsmethode** aus. Damit geben Sie an, ob die Volume-Daten vollständig aus dem Workload auf die Failover-VM übertragen oder mit Volumes auf einer vorhandenen VM synchronisiert werden sollen. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (vollständig und inkrementell)“, auf Seite 86.
5. Weisen Sie ein Schutzziel zu. Dies kann entweder ein Container oder ein **vorbereiteter** Workload sein, falls Sie *Inkrementelle Reproduktion* als anfängliche Reproduktionsmethode ausgewählt haben. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (vollständig und inkrementell)“, auf Seite 86.

   HINWEIS: Wenn Ihr Inventar nur einen Container enthält, wird diesem Ihr Workload automatisch zugewiesen.

   ---

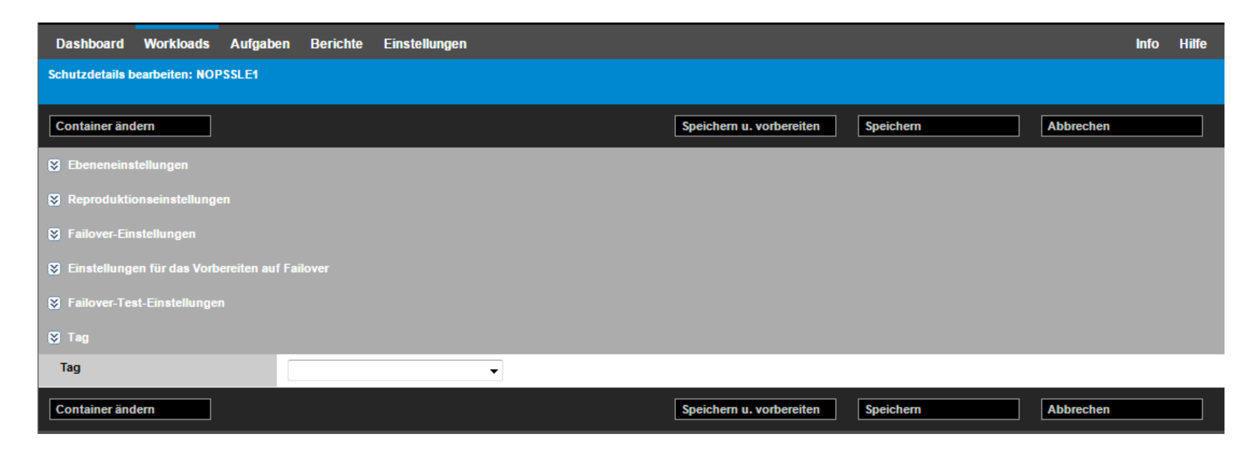
6. Konfigurieren Sie die Schutzdetails in jeder Einstellungsgruppe so, wie sie für die Aufrechterhaltung Ihres ununterbrochenen Geschäftsbetriebs erforderlich sind. Weitere Informationen hierzu finden Sie unter „Workload-Schutz-Details“, auf Seite 62.
7. Korrigieren Sie alle Validierungsfehler, die eventuell auf der PlateSpin Protect-Weboberfläche angezeigt werden.
8. Klicken Sie auf **Speichern**.

Sie können alternativ auch auf **Speichern und vorbereiten** klicken. Dies speichert die Einstellungen und führt gleichzeitig den Befehl **Reproduktion vorbereiten** aus (bei Bedarf werden Datenübertragungstreiber auf dem Ursprungs-Workload installiert und die anfängliche VM-Reproduktion Ihres Workloads wird erstellt).

Warten Sie, bis der Vorgang abgeschlossen ist. Anschließend wird das Ereignis **Workload-Konfiguration abgeschlossen** im Dashboard angezeigt.

4.4.1 Workload-Schutz-Details

Workload-Schutz-Details werden in fünf Parametergruppen angegeben:



Sie können jede Parametergruppe erweitern oder komprimieren, indem Sie auf das -Symbol auf der linken Seite klicken.

Im Folgenden sind die Details der fünf Parametergruppen aufgeführt:

***Tabelle 4-1** Workload-Schutz-Details*

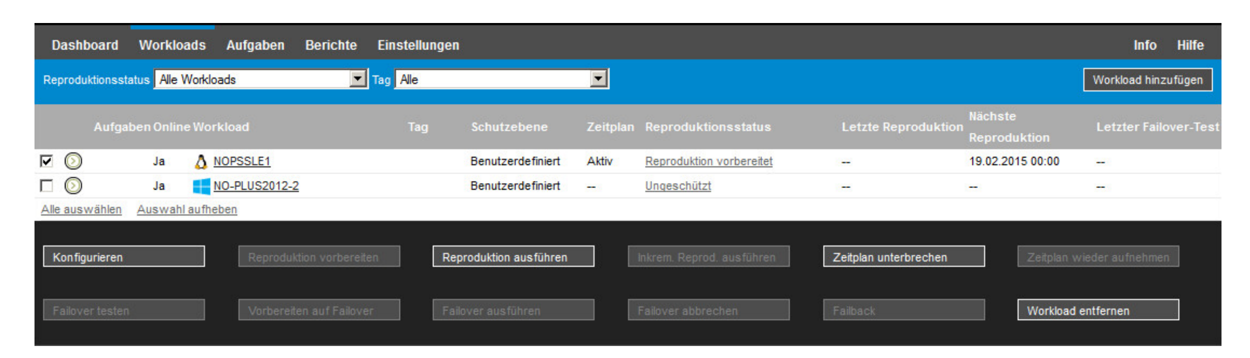
Parametergruppe (Einstellungen)	Details
Ebene	Gibt die Schutzebene des aktuellen Schutzes an. Weitere Informationen hierzu finden Sie unter „Schutzebenen“, auf Seite 84.

Parametergruppe (Einstellungen)	Details
Reproduktion	**Übertragungsmethode:** (Windows) Wählen Sie eine Datenübertragungsmethode und Sicherheit durch Verschlüsselung aus. Weitere Informationen hierzu finden Sie unter „Datenübertragung“, auf Seite 83. **Übertragungsverschlüsselung:** Wählen Sie zum Aktivieren der Verschlüsselung die Option **Datenübertragung verschlüsseln**. Weitere Informationen hierzu finden Sie in „Sicherheit und Datenschutz“, auf Seite 18. **Ursprungsberechtigungsnachweis:** Für den Zugriff auf den Workload erforderlich. Weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 76. **Anzahl der CPUs:** Geben Sie die erforderliche Anzahl der vCPUs an, die dem Failover-Workload zugewiesen wurden (gilt nur dann, wenn Sie **Vollständig** als Methode der ursprünglichen Reproduktion ausgewählt haben). **Reproduktionsnetzwerk:** Ermöglicht die Trennung des Reproduktionsdatenverkehrs auf der Basis virtueller Netzwerke, die in Ihrem VM-Container definiert sind. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 90. Für diese Einstellung können Sie außerdem einen MTU-Wert festlegen, der vom LRD-Reproduktionsnetzwerk (Linux RAM Disk) in PlateSpin Protect verwendet werden soll. Dieser Wert kann dazu beitragen, übermäßigen Datenverkehr über Netzwerke (z. B. VPNs) mit kleinerem MTU-Wert zu vermeiden. Der Standardwert ist eine leere Zeichenkette (kein Eintrag im Textfeld). Wenn Networking im LRD konfiguriert ist, kann das Netzwerkgerät einen eigenen Standardwert festlegen (in der Regel 1500). Wenn Sie einen Wert eingeben, passt PlateSpin Protect den MTU-Wert beim Konfigurieren der Netzwerkschnittstelle entsprechend an. **Zulässige Netzwerke:** Gibt mindestens eine Netzwerkschnittstelle (NIC oder IP-Adresse) am Ursprung für den Reproduktionsdatenverkehr an. **Ressourcenpool für Ziel-VM:** (Einstellung nur dann verfügbar, wenn der Container ein DRS-Cluster ist.) Speicherort des Ressourcenpools, an dem die Failover-VM im Protect-Container erstellt werden soll. **VM-Ordner für Ziel-VM:** (Einstellung nur dann verfügbar, wenn der Container ein DRS-Cluster ist.) Speicherort des VM-Ordners, an dem die Failover-VM im Protect-Container erstellt werden soll. **Konfigurationsdatei-Datenablage:** Ermöglicht die Auswahl einer mit dem VM-Container verbundenen Datenablage zum Speichern von VM-Konfigurationsdateien. Weitere Informationen hierzu finden Sie unter „Wiederherstellungspunkte“, auf Seite 86. **Geschützte Volumes:** Verwenden Sie diese Optionen, um Volumes für den Schutz auszuwählen und deren Reproduktionen spezifischen Datenablagen im VM-Container zuzuweisen. **Thin-Festplatten-Option:** Aktiviert die Funktion für virtuelle Thin-Provisioned-Datenträger, bei der ein virtueller Datenträger für den virtuellen Computer eine feste Größe zu haben scheint, jedoch nur die Menge an Festplattenspeicher verbraucht, die tatsächlich von den Daten auf diesem Datenträger benötigt wird. **Geschützte logische Volumes:** Gibt die logischen LVM-Volumes an, die für einen Linux-Workload oder die NSS-Pools in einem OES-Workload geschützt werden sollen.

Parametergruppe (Einstellungen)	Details
	Speicher ohne Volumes: Gibt einen Ablagebereich (z. B. eine Auslagerungspartition) an, der mit dem Ursprungs-Workload verbunden ist. Dieser Speicher wird im Failover-Workload erneut erstellt. **Volume-Gruppen:** In Linux bestimmt diese Einstellung die LVM-Volume-Gruppen, die mit den unter Geschützte logische Volumes in den Einstellungen angegebenen logischen LVM-Volumes geschützt werden sollen. **Dienste/Daemons, die während der Reproduktion angehalten werden sollen:** Ermöglicht die Auswahl von Windows-Services oder Linux-Daemons, die während der Reproduktion automatisch angehalten werden sollen. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 87.
Failover	**VM-Arbeitsspeicher:** Gibt die Menge an Arbeitsspeicher an, die dem Failover-Workload zugeteilt werden soll. **Hostname und Domänen-/Arbeitsgruppenzugehörigkeit:** Verwenden Sie diese Optionen, um die Identität und Domänen-/Arbeitsgruppenzugehörigkeit des Failover-Workloads zu steuern, wenn dieser „live“ ist. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich. **Netzwerkverbindungen:** Verwenden Sie diese Optionen, um die LAN-Einstellungen des Failover-Workloads festzulegen. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 90. **Zu ändernde Dienst/Daemon-Status:** Ermöglicht Ihnen die Steuerung des Anfangsstatus spezifischer Anwendungsdienste (Windows) oder Daemons (Linux). Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 87.
Vorbereiten auf Failover	Ermöglicht Ihnen die Steuerung der temporären Netzwerkeinstellungen des Failover-Workloads während des optionalen Vorgangs der Vorbereitung auf den Failover. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 90.
Failover testen	**VM-Arbeitsspeicher:** Ermöglicht Ihnen das Zuweisen des erforderlichen RAM zum temporären Workload. **Hostname:** Ermöglicht Ihnen das Zuweisen eines Hostnamens zum temporären Workload. **Domäne/Arbeitsgruppe:** Ermöglicht Ihnen die Zuordnung des temporären Workloads zu einer Domäne oder Arbeitsgruppe. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich. **Netzwerkverbindungen:** Steuert die LAN-Einstellungen des temporären Workloads. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 90. **Zu ändernde Dienst/Daemon-Status:** Ermöglicht Ihnen die Steuerung des Anfangsstatus spezifischer Anwendungsdienste (Windows) oder Daemons (Linux). Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 87.

4.5 Starten des Workload-Schutzes

Der Workload-Schutz wird durch den Befehl **Reproduktion ausführen** gestartet:



Sie können den Befehl „Reproduktion ausführen“ nach folgenden Aktionen ausführen:

- Hinzufügen eines Workloads.
- Konfigurieren der Schutzdetails eines Workloads.
- Vorbereiten der anfänglichen Reproduktion.

Wenn Sie bereit sind, fortzufahren:

1. Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus und klicken Sie auf **Reproduktion ausführen**.
2. Klicken Sie auf **Ausführen**.

   PlateSpin Protect startet die Ausführung und zeigt eine Fortschrittsanzeige ( ) für den Schritt **Daten kopieren** an.

HINWEIS: Nachdem ein Workload geschützt wurde:

- Das Ändern der Größe eines Volumes, das auf Blockebene geschützt wird, macht den Schutz ungültig. Gehen Sie wie folgt vor: 1. Entfernen Sie den Workload aus dem Schutz. 2. Ändern Sie die Größe der Volumes wie erforderlich. 3. Bauen Sie den Schutz erneut auf, indem Sie den Workload erneut hinzufügen, dessen Schutzdetails konfigurieren und die Reproduktionen starten.
- Nach jeder signifikanten Änderung des geschützten Workloads muss der Schutz neu hergestellt werden. Dies ist zum Beispiel erforderlich, wenn Volumes oder Netzwerkkarten zu einem geschützten Workload hinzugefügt wurden.

4.6 Abbrechen von Befehlen

Auf der Seite „Befehlsdetails“ eines bestimmten Befehls können sie diesen nach dessen Ausführung abbrechen, solange er noch nicht durchgeführt wurde.

So greifen Sie auf die Seite „Befehlsdetails“ eines Befehls zu, der noch nicht durchgeführt wurde:

1. Wechseln Sie zur Seite „Workloads“.
2. Suchen Sie den erforderlichen Workload, und klicken Sie auf den Link für den Befehl, der gerade auf diesem Workload ausgeführt wird, beispielsweise **Inkrementelle Reproduktion wird durchgeführt**.

Auf der PlateSpin Protect-Weboberfläche wird die entsprechende Seite „Befehlsdetails“ angezeigt:



3 Klicken Sie auf **Abbrechen**.

4.7 Failover

Ein *Failover* hat zur Folge, dass die Business-Funktion eines ausgefallenen Workloads von einem Failover-Workload innerhalb eines PlateSpin Protect-VM-Containers übernommen wird.

- Abschnitt 4.7.1, „Erkennen von Offline-Workloads“, auf Seite 66
- Abschnitt 4.7.2, „Durchführen eines Failovers“, auf Seite 67
- Abschnitt 4.7.3, „Verwenden der Funktion „Failover testen““, auf Seite 67

4.7.1 Erkennen von Offline-Workloads

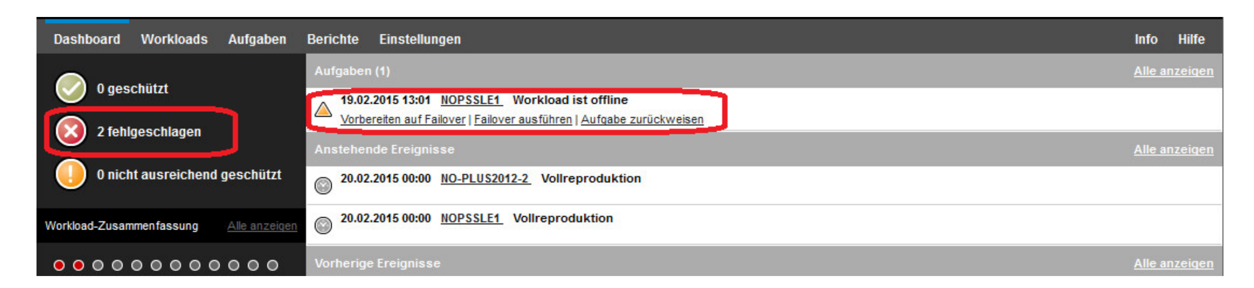
PlateSpin Protect überwacht ständig Ihre geschützten Workloads. Wenn ein Versuch zur Überwachung eines Workloads so oft wie vorher festgelegt fehlschlägt, generiert PlateSpin Protect das Ereignis **Workload ist offline**. Kriterien, anhand derer ein Workload-Fehler definiert und protokolliert wird, sind Teil der Ebeneneinstellungen eines Workload-Schutzes (Informationen hierzu finden Sie in der Zeile Ebene unter „Workload-Schutz-Details“, auf Seite 62).

Wenn zusammen mit den SMTP-Einstellungen Benachrichtigungen konfiguriert wurden, sendet PlateSpin Protect gleichzeitig eine Benachrichtigungs-Email an die angegebenen Empfänger. Weitere Informationen hierzu finden Sie in „Einrichten automatischer Email-Benachrichtigungen zu Ereignissen und Berichten“, auf Seite 35.

Wenn ein Workload-Fehler erkannt wird, während der Status der Reproduktion **Im Leerlauf** lautet, können Sie mit dem Befehl **Failover ausführen** fortfahren. Wenn ein Workload-Fehler auftritt, während eine inkrementelle Reproduktion stattfindet, bleibt der Vorgang hängen. Brechen Sie in diesem Fall den Vorgang ab (weitere Informationen hierzu finden Sie unter „Abbrechen von Befehlen“, auf Seite 65) und fahren Sie dann mit dem Befehl **Failover ausführen** fort. Weitere Informationen hierzu finden Sie unter „Durchführen eines Failovers“, auf Seite 67.

Die folgende Abbildung zeigt die Dashboard-Seite der PlateSpin Protect-Weboberfläche beim Erkennen eines Workload-Fehlers. Beachten Sie die anwendbaren Aufgaben im Teilfenster mit den Aufgaben und Ereignissen:

***Abbildung 4-1** Die Dashboard-Seite bei Erkennen eines Workload-Fehlers („Workload offline“)*



4.7.2 Durchführen eines Failovers

Failover-Einstellungen, einschließlich der Netzwerkidentitäts- und LAN-Einstellungen des Failover-Workloads, werden zum Zeitpunkt der Konfiguration zusammen mit den Schutzdetails gespeichert. Informationen hierzu finden Sie in der Zeile Failover unter „Workload-Schutz-Details“, auf Seite 62.

Sie können folgende Methoden zur Durchführung eines Failovers verwenden:

- Wählen Sie den erforderlichen Workload auf der Seite „Workloads“ aus und klicken Sie auf **Failover ausführen**.
- Klicken Sie auf den entsprechenden Befehls-Hyperlink im Ereignis **Workload ist offline** im Teilfenster mit den Aufgaben und Ereignissen. Weitere Informationen hierzu finden Sie unter Abbildung 4-1.
- Führen Sie einen Befehl **Auf Failover vorbereiten** aus, um den virtuellen Failover-Computer rechtzeitig vorher zu booten. Sie können den Failover danach auch immer wieder abbrechen (was bei stufenweisen Failovers nützlich ist).

Verwenden Sie eine dieser Methoden, um den Failover-Vorgang zu starten, und wählen Sie einen Wiederherstellungspunkt aus, der auf den Failover-Workload angewendet werden soll (Informationen hierzu finden Sie unter „Wiederherstellungspunkte“, auf Seite 86). Klicken Sie auf **Ausführen** und überwachen Sie den Vorgang. Wenn der Vorgang abgeschlossen ist, sollte der Reproduktionsstatus des Workloads **Live** lauten.

Informationen zum Testen des Failover-Workloads oder des Failover-Vorgangs im Rahmen einer geplanten Übung zur Wiederherstellung im Katastrophenfall finden Sie unter „Verwenden der Funktion „Failover testen““, auf Seite 67.

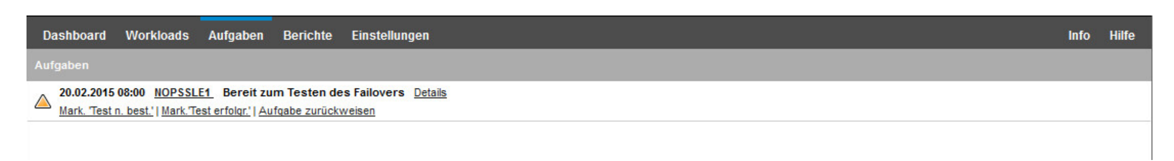
4.7.3 Verwenden der Funktion „Failover testen“

PlateSpin Protect ermöglicht es Ihnen, die Failover-Funktionalität und die Integrität des Failover-Workloads zu testen. Dies geschieht unter Verwendung des Befehls **Failover testen**, der den Failover-Workload zu Testzwecken in einer eingeschränkten Netzwerkumgebung bootet.

Wenn Sie diesen Befehl ausführen, wendet PlateSpin Protect die Failover-Test-Einstellungen, die in den Workload-Schutz-Details gespeichert sind, auf den Failover-Workload an (siehe Zeile Failover testen in „Workload-Schutz-Details“, auf Seite 62.

1. Definieren Sie ein angemessenes Zeitfenster für das Testen, und stellen Sie sicher, dass keine Reproduktionen im Gange sind. Der Reproduktionsstatus des Workload muss **Im Leerlauf** sein.
2. Wählen Sie auf der Seite „Workloads“ den erforderlichen Workload aus, klicken Sie auf **Failover testen**, wählen Sie einen Wiederherstellungspunkt aus (siehe „Wiederherstellungspunkte“, auf Seite 86) und klicken Sie anschließend auf **Ausführen**.

   Anschließend generiert PlateSpin Protect ein entsprechendes Ereignis sowie eine Aufgabe mit einem Satz von anwendbaren Befehlen:

3. Überprüfen Sie die Integrität und die Betriebsfunktionen des Failover-Workloads. Verwenden Sie den VMware vSphere-Client, um auf den Failover-Workload im VM-Container zuzugreifen.

4 Markieren Sie den Test als **nicht bestanden** oder **erfolgreich bestanden**. Verwenden Sie die entsprechenden Befehle in der Aufgabe (**Mark. 'Test n. best.'**, **Mark. 'Test erfolgr.'**). Die ausgewählte Aktion wird im Verlauf der Ereignisse gespeichert, die mit dem Workload verknüpft sind und kann über Berichte abgerufen werden. **Aufgabe zurückweisen** verwirft die Aufgabe und das Ereignis.

   Nach Abschluss der Aufgaben **Mark. 'Test n. best.'** oder **Mark. 'Test erfolgr.'** verwirft PlateSpin Protect die temporären Einstellungen, die auf den Failover-Workload angewendet wurden. Der Schutz wird in den Zustand versetzt, den er vor dem Test hatte.

4.8 Failback

Der nächste logische Schritt, der einem Failover folgt, ist ein Failback-Vorgang. Er überträgt den Failover-Workload an seine ursprüngliche oder, falls erforderlich, auf eine neue Infrastruktur.

Unterstützte Failback-Methoden hängen vom Typ der Zielinfrastruktur und dem Grad der Automatisierung des Failback-Vorgangs ab:

- **Automatischer Failback auf eine virtuelle Maschine:** Unterstützt für VMware ESX-Plattformen und VMware DRS-Cluster.
- **Halbautomatischer Failback auf einen physischen Computer:** Wird für alle physischen Computer unterstützt.
- **Halbautomatischer Failback auf eine virtuelle Maschine:** Wird für Microsoft Hyper-V-Plattformen unterstützt.

Die folgenden Abschnitte enthalten weitere Informationen:

- Abschnitt 4.8.1, „Automatischer Failback auf eine VM-Plattform“, auf Seite 68
- Abschnitt 4.8.2, „Halbautomatischer Failback auf einen physischen Computer“, auf Seite 71
- Abschnitt 4.8.3, „Halbautomatischer Failback auf eine virtuelle Maschine“, auf Seite 72

4.8.1 Automatischer Failback auf eine VM-Plattform

Die folgenden Container werden als Ziele für automatische Failbacks unterstützt:

Ziel	Haftnotizen
VMware DRS-Cluster in vSphere 5.15	• Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) • Als VM-Container darf der DRS-Cluster nur aus ESXi 5.5-Servern bestehen und kann nur von vCenter 5.5 verwaltet werden.
VMware DRS-Cluster in vSphere 5.1	• Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) • Als VM-Container darf der DRS-Cluster nur aus ESXi 5.1-Servern bestehen und kann nur von vCenter 5.1 verwaltet werden.
VMware DRS-Cluster in vSphere 5.0	• Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) • Als VM-Container darf der DRS-Cluster nur aus ESXi 5.0-Servern bestehen und kann nur von vCenter 5.0 verwaltet werden.

Ziel	Haftnotizen
VMware DRS-Cluster in vSphere 4.1	◆ Die DRS-Konfiguration muss entweder **Teilweise automatisiert** oder **Vollautomatisch** sein (sie darf nicht auf **Manuell** gesetzt sein) ◆ Als VM-Container kann der Cluster – da er ein Container ist – eine Kombination aus ESX 4.1- und ESX**i** 4.1-Servern verwenden und kann nur von vCenter 4.1 verwaltet werden
VMware ESX**i** 4.1, 5.0, 5.1	ESX**i**-Versionen erfordern eine erworbene Lizenz. Der Schutz wird bei diesen Systemen nicht unterstützt, wenn sie mit einer kostenlosen Lizenz ausgeführt werden.
VMware ESX 4.1	

Führen Sie folgende Schritte aus, um einen automatischen Failback eines Failover-Workloads auf einen Ziel-VMware-Container durchzuführen.

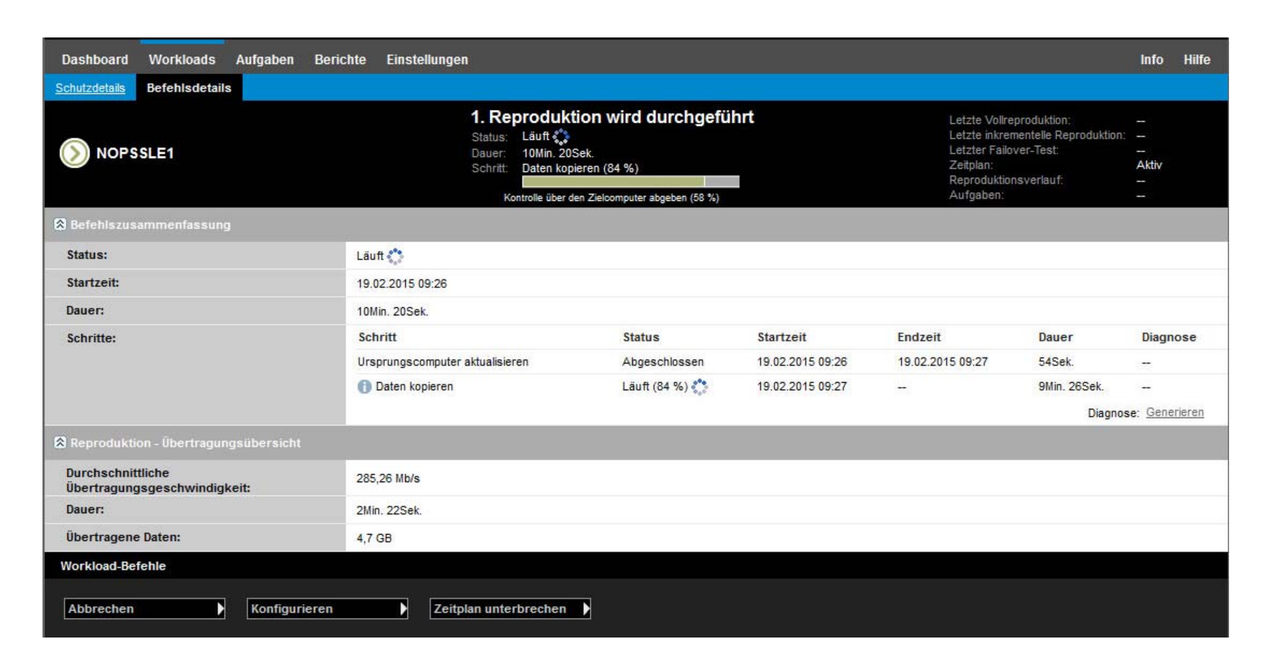
1. Wählen Sie im Anschluss an einen Failover den Workload auf der Seite „Workloads“ aus und klicken Sie auf **Failback durchführen**.

   Sie werden aufgefordert, die nachfolgenden Auswahlen zu treffen.
2. Legen Sie die folgenden Parametergruppen fest:
   - **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Failover-Workloads und den Berechtigungsnachweis eines Administrators an. Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 76).
   - **Failback-Zieleinstellungen:** Geben Sie die folgenden Parameter an:
     - **Reproduktionsmethode:** Wählen Sie den Umfang der Datenreproduktion aus. Wenn Sie **Inkrementell** auswählen, müssen Sie ein Ziel **vorbereiten**. Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (vollständig und inkrementell)“, auf Seite 86.
     - **Zieltyp:** Wählen Sie **Virtuelles Ziel** aus. Falls Sie nicht über einen Failback-Container verfügen, klicken Sie auf **Container hinzufügen** und inventarisieren Sie einen unterstützten Container.
3. Klicken Sie auf **Speichern und vorbereiten** und überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

   Nach erfolgreichem Abschluss lädt PlateSpin Protect den Bildschirm „Bereit für Failback“ und fordert Sie auf, die Details des Failback-Vorgangs anzugeben.
4. Konfigurieren Sie die Failback-Details. Weitere Informationen hierzu finden Sie unter „Failback-Details (Workload an VM)“, auf Seite 70.
5. Klicken Sie auf **Speichern und Failback durchführen** und überwachen Sie den Fortschritt auf der Seite „Befehlsdetails“. Weitere Informationen hierzu finden Sie unter Abbildung 4-2.

   PlateSpin Protect führt den Befehl aus. Wenn Sie in der Parametergruppe „Post-Failback“ die Option **Erneut schützen nach Failback** ausgewählt haben, wird der Befehl **Erneut schützen** auf der PlateSpin Protect-Weboberfläche angezeigt.

Abbildung 4-2 Failback-Befehlsdetails



Failback-Details (Workload an VM)

Failback-Details werden durch drei Parametergruppen dargestellt, die Sie konfigurieren, wenn Sie einen Workload-Failback an eine virtuelle Maschine durchführen.

Tabelle 4-2 Failback-Details (VM)

Parametergruppe (Einstellungen)	Details
Failback	**Übertragungsmethode:** Ermöglicht Ihnen, eine Datenübertragungsmethode und Sicherheit durch Verschlüsselung auszuwählen. Weitere Informationen hierzu finden Sie unter „Datenübertragung“, auf Seite 83. **Failback-Netzwerk:** Ermöglicht Ihnen, den Failback-Datenverkehr über ein dediziertes Netzwerk zu leiten, das zu den in Ihrem VM-Container definierten Netzwerken gehört. Weitere Informationen hierzu finden Sie unter „Netzwerke“, auf Seite 90. **VM-Datenablage:** Ermöglicht Ihnen die Auswahl einer Datenablage, die Ihrem Failback-Container für den Ziel-Workload zugeordnet ist. **Volume-Zuordnung:** Wenn Sie als anfängliche Reproduktionsmethode die Option „Inkrementell“ ausgewählt haben, können Sie hier die Ursprungs-Volumes auswählen und dem Failback-Ziel zur Synchronisierung zuordnen. **Anzuhaltende Dienste/Daemons:** Ermöglicht Ihnen die Auswahl von Windows-Diensten oder Linux-Daemons, die während des Failbacks automatisch angehalten werden sollen. Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 87. **Alternative Adresse für Ursprung:** Hier kann ggf. eine zusätzliche IP-Adresse für den virtuellen Failover-Computer eingegeben werden. Weitere Informationen hierzu finden Sie unter „Schutz über öffentliche und private Netzwerke durch NAT“, auf Seite 33.

Parametergruppe (Einstellungen)	Details
Workload	**Anzahl der CPUs:** Ermöglicht Ihnen die Angabe der erforderlichen Anzahl der dem Ziel-Workload zugewiesenen vCPUs. **VM-Arbeitsspeicher:** Ermöglicht Ihnen das Zuweisen des erforderlichen RAM zum Ziel-Workload. **Hostname, Domäne/Arbeitsgruppe:** Verwenden Sie diese Optionen, um die Identität und Domänen-/Arbeitsgruppenzugehörigkeit des Ziel-Workloads zu steuern. Für die Domänenzugehörigkeit ist der Berechtigungsnachweis eines Domänenadministrators erforderlich. **Netzwerkverbindungen:** Verwenden Sie diese Optionen, um die Netzwerkzuordnung des Ziel-Workloads basierend auf den virtuellen Netzwerken des zugrunde liegenden VM-Containers anzugeben. **Zu ändernde Dienststatus:** Ermöglicht Ihnen die Steuerung des Anfangsstatus spezifischer Anwendungsdienste (Windows) oder Daemons (Linux). Weitere Informationen hierzu finden Sie unter „Steuerung von Diensten und Daemons“, auf Seite 87.
Post-Failback	**Workload erneut schützen:** Verwenden Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload nach der Bereitstellung neu zu erstellen. Dadurch kann der Ereignisverlauf für den Workload kontinuierlich geführt und eine Workload-Lizenz automatisch zugewiesen/festgelegt werden. ◆ **Erneut schützen nach Failback:** Wählen Sie diese Option, wenn Sie planen, den Schutzvertrag für den Ziel-Workload neu zu erstellen. Wenn der Failback abgeschlossen ist, steht für den Failback-Workload der Befehl **Erneut schützen** auf der PlateSpin Protect-Weboberfläche zur Verfügung. ◆ **Kein erneutes Schützen:** Wählen Sie diese Option, wenn Sie den Schutzvertrag für den Ziel-Workload nicht neu erstellen möchten. Zum Schützen des Failback-Workload nach dessen Abschluss müssen Sie diesen Workload neu inventarisieren und dessen Schutzdetails neu konfigurieren.

4.8.2 Halbautomatischer Failback auf einen physischen Computer

Gehen Sie folgendermaßen vor, um nach einem Failover den Failback eines Workloads an einen physischen Computer durchzuführen. Bei dem physischen Computer kann es sich um die ursprüngliche oder eine neue Infrastruktur handeln.

1. Registrieren Sie den erforderlichen physischen Computer bei Ihrem PlateSpin-Server. Weitere Informationen hierzu finden Sie unter „Failback auf physische Computer“, auf Seite 90.
2. Falls Treiber fehlen oder nicht kompatibel sind, laden Sie die erforderlichen Treiber in die Gerätetreiberdatenbank von PlateSpin Protect hoch. Weitere Informationen hierzu finden Sie unter „Verwalten der Gerätetreiber“, auf Seite 99.
3. Wählen Sie im Anschluss an einen Failover den Workload auf der Seite „Workloads“ aus und klicken Sie auf **Failback durchführen**.
4. Legen Sie die folgenden Parametergruppen fest:
   - **Workload-Einstellungen:** Geben Sie den Hostnamen oder die IP-Adresse Ihres Failover-Workloads und den Berechtigungsnachweis eines Administrators an. Verwenden Sie das erforderliche Berechtigungsnachweisformat (weitere Informationen hierzu finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 76).

- **Failback-Zieleinstellungen:** Geben Sie die folgenden Parameter an:
    - **Reproduktionsmethode:** Wählen Sie den Umfang der Datenreproduktion aus.

      Weitere Informationen hierzu finden Sie unter „Anfängliche Reproduktionsmethode (vollständig und inkrementell)“, auf Seite 86.
    - **Zieltyp:** Wählen Sie die Option **Physische Ziele** und wählen Sie anschließend den physischen Computer aus, den Sie in Schritt 1 registriert haben.

5. Klicken Sie auf **Speichern und vorbereiten** und überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

   Nach erfolgreichem Abschluss lädt PlateSpin Protect den Bildschirm „Bereit für Failback“ und fordert Sie auf, die Details des Failback-Vorgangs anzugeben.
6. Konfigurieren Sie die Failback-Details und klicken Sie anschließend auf **Speichern und Failback durchführen**.

   Überwachen Sie den Fortschritt auf dem Bildschirm „Befehlsdetails“.

4.8.3 Halbautomatischer Failback auf eine virtuelle Maschine

Bei diesem Failback-Typ wird ein Prozess ähnlich dem Halbautomatischer Failback auf einen physischen Computer für ein VM-Ziel durchgeführt, das kein nativ unterstützter VMware-Container ist. Während dieses Prozesses weisen Sie das System an, ein VM-Ziel als physischen Computer zu betrachten.

Sie können einen halbautomatischen Failback an einem Container vornehmen, der einen vollautomatischen Failback unterstützt (VMware ESX- und DRS-Cluster-Ziele).

Sie können auch einen halbautomatischen Failback an Ziel-VM-Plattformen auf Microsoft Hyper-V-Server-Hosts vornehmen.

So starten Sie die Hyper-V-VMs bei einem Failover:

1. Fügen Sie in einem Texteditor jeweils die folgende Zeile in die Datei `/etc/vmware/config` der einzelnen Hyper-V-Hosts ein:

   ```
   vhv.allow = "TRUE"
   ```
2. Bearbeiten Sie im vSphere-Web-Client die Failover-VM-Einstellungen für die CPU:

   2a Wählen Sie auf der Registerkarte **Virtuelle Hardware** die Option **CPU**.

   2b Wählen Sie unter **Hardware-Virtualisierung** die Option **Hardwaregestützte Virtualisierung für Gast-Betriebssystem offenlegen**.
3. Bearbeiten Sie im vSphere-Web-Client die Failover-VM-Einstellungen für die CPU-ID:

   3a Erweitern Sie auf der Registerkarte **VM-Optionen** den Eintrag **Erweitert**, und wählen Sie die Option **Konfigurationsparameter bearbeiten**.

   3b Überprüfen Sie die folgende Einstellung:

   ```
   hypervisor.cpuid.v0 = FALSE
   ```

4.9 Erneutes Schützen eines Workloads

Durch den Vorgang **Erneut schützen**, dem logischen nächsten Schritt nach einem **Failback** wird der Workload-Schutz-Lebenszyklus abgeschlossen und neu gestartet. Nach einem erfolgreichen Failback-Vorgang wird ein Befehl **Erneut schützen** auf der PlateSpin Protect-Weboberfläche zur Verfügung gestellt und das System wendet die gleichen Schutzdetails an wie bereits bei der ursprünglichen Konfiguration des Schutzvertrags angegeben.

HINWEIS: Der Befehl **Erneut schützen** ist nur verfügbar, wenn Sie die Option **Erneut schützen** in den Failback-Details ausgewählt haben. Weitere Informationen hierzu finden Sie unter „Failback“, auf Seite 68.

Der restliche Workflow im Schutz-Lebenszyklus ist der gleiche wie der bei normalen Vorgängen zum Workload-Schutz. Sie können ihn so oft wie erforderlich wiederholen.

5 Grundlagen des Workload-Schutzes

Dieser Abschnitt bietet Informationen zu den verschiedenen funktionalen Bereichen eines Workload-Schutzvertrags.

5.1 Workload-Lizenzverbrauch

Die PlateSpin Protect-Produktlizenz berechtigt Sie für eine bestimmte Anzahl von Workloads zum Schutz durch die Workload-Lizenzierung. Jedes Mal, wenn Sie einen zu schützenden Workload hinzufügen, verbraucht das System eine einzelne Workload-Lizenz aus Ihrem Lizenzpool. Sie können eine verbrauchte Lizenz durch Entfernen eines Workloads bis zu maximal fünf Mal wiederherstellen.

Informationen über die Produktlizenzierung und die Lizenzaktivierung finden Sie unter „Produktlizenzierung“, auf Seite 23.

5.2 Richtlinien für Workload- und Container-Berechtigungsnachweise

PlateSpin Protect muss über Zugriff auf Workloads auf Administratorebene sowie eine entsprechende Rollenkonfiguration für Container verfügen. Während des gesamten Workload-Schutz- und -Wiederherstellungs-Workflows werden Sie von PlateSpin Protect aufgefordert, Berechtigungsnachweise in einem bestimmten Format einzugeben.

Tabelle 5-1 *Workload- und Container-Berechtigungsnachweise*

Ermitteln	Berechtigungsnachweis	Anmerkungen
Alle Windows-Workloads	Berechtigungsnachweise eines lokalen oder Domänen-Administrators.	Verwenden Sie für den Benutzernamen das folgende Format: ◆ Bei Domänenmitgliedscomputern: *Autorität**Prinzipal* ◆ Bei Arbeitsgruppenmitgliedscomputern: *Hostname**Prinzipal*
Windows-Cluster	Berechtigungsnachweis eines Domänen-Administrators.	
Alle Linux-Workloads	Root-äquivalenter Benutzername und Passwort	Andere Konten als das Root-Konto müssen für die Verwendung von `sudo` konfiguriert werden. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7920711.
VMware ESX/ESXi 4.1; ESXi 5.0, ESXi 5.1, ESXi 5.5	VMware-Konto mit einer entsprechenden Rollenkonfiguration. Weitere Informationen hierzu finden Sie unter Abschnitt 5.3.1, „Verwenden von Werkzeugen zum Definieren von VMware-Rollen“, auf Seite 77.	Wenn ESX für die Windows-Domänenauthentifizierung konfiguriert ist, können Sie auch Ihren Berechtigungsnachweis für die Windows-Domäne verwenden.
VMware vCenter Server	VMware-Konto mit einer entsprechenden Rollenkonfiguration. Weitere Informationen hierzu finden Sie unter Abschnitt 5.3.1, „Verwenden von Werkzeugen zum Definieren von VMware-Rollen“, auf Seite 77.	

5.3 Einrichten der Protect-Mehrmandantenfähigkeit auf VMWare

PlateSpin Protect enthält eindeutige Benutzerrollen (und ein Werkzeug für deren Erstellung in einem VMware-Rechenzentrum), die es VMware-Benutzern ohne Administratorrechte (oder „aktivierten Benutzern“) ermöglicht, Protect-Lebenszyklusvorgänge in der VMware-Umgebung auszuführen. Anhand dieser Rollen können Sie als Dienstanbieter Ihren VMware-Cluster für eine Mehrfachmandantenfähigkeit segmentieren. Dies bedeutet, dass mehrere Protect-Container in Ihrem

Rechenzentrum instanziiert werden, um Protect-Kunden oder „Mandanten“ aufzunehmen, die ihre Daten und den Nachweis über deren Vorhandensein von anderen Kunden, die ebenfalls Ihr Rechenzentrum nutzen, getrennt halten und den Zugriff durch diese Kunden verhindern möchten.

Dieser Abschnitt enthält folgende Informationen:

- Abschnitt 5.3.1, „Verwenden von Werkzeugen zum Definieren von VMware-Rollen“, auf Seite 77
- Abschnitt 5.3.2, „Zuweisen von Rollen in vCenter“, auf Seite 79

5.3.1 Verwenden von Werkzeugen zum Definieren von VMware-Rollen

PlateSpin Protect erfordert bestimmte Berechtigungen für den Zugriff auf und die Durchführung von Aufgaben in der VMware-Infrastruktur (also VMware-„Container“), die den Protect-Workflow und die Protect-Funktionen in dieser Umgebung ermöglichen. Da diese erforderlichen Berechtigungen sehr zahlreich sind, hat NetIQ eine Datei erstellt, die die mindestens erforderlichen Berechtigungen definiert und diese in drei benutzerdefinierten VMware-Rollen entsprechend zusammenfasst:

- PlateSpin-Manager für virtuelle Maschinen
- PlateSpin-Infrastruktur-Manager
- PlateSpin-Benutzer

Diese Definitionsdatei (`PlateSpinRole.xml`) ist in der Installation des PlateSpin Protect-Servers enthalten. Über eine zusätzliche ausführbare Datei (`PlateSpin.VMwareRoleTool.exe`) kann auf die Datei zugegriffen werden, um die Erstellung dieser benutzerdefinierten PlateSpin-Rollen in einer vCenter-Zielumgebung zu ermöglichen.

Dieser Abschnitt enthält folgende Informationen:

- „Grundlegende Befehlszeilensyntax“, auf Seite 77
- „Zusätzliche Befehlszeilenparameter und -flaggen“, auf Seite 77
- „Beispiel für die Verwendung des Werkzeugs“, auf Seite 78
- „(Optional) Manuelle Definition der PlateSpin-Rollen in vCenter“, auf Seite 78

Grundlegende Befehlszeilensyntax

Führen Sie am Standort, an dem das Rollenwerkzeug installiert wurde, das Werkzeug an der Befehlszeile aus und verwenden Sie dazu diese grundlegende Syntax:

```
PlateSpin.VMwareRoleTool.exe /host=[host name/IP] /user=[user name] /role=[the
role definition file name and location] /create
```

HINWEIS: Die Datei mit der Rollendefinition befindet sich standardmäßig im Ordner mit dem Rollendefinitionswerkzeug.

Zusätzliche Befehlszeilenparameter und -flaggen

Wenden Sie nach Bedarf die folgenden Parameter an, wenn Sie die `PlateSpin.VMwareRoleTool.exe` zur Erstellung oder Aktualisierung in vCenter verwenden:

`/Erstellen`	(Obligatorisch) Erstellt die Rollen, die durch den Parameter `/Rolle` definiert wurde
`/Alle_Berechtigungen_abrufen`	Zeigt alle vom Server definierten Berechtigungen an
Optionale Flaggen	
`/Interaktiv`	Führen Sie das Werkzeug mit interaktiven Optionen aus, anhand derer Sie einzelne Rollen wählen, die Rollenkompatibilität überprüfen oder alle kompatiblen Rollen auflisten können.
`/password=[passwort]`	Gibt das VMware-Passwort an (umgeht die Aufforderung zur Eingabe des Passworts)
`/verbose`	Zeigt detaillierte Informationen an

Beispiel für die Verwendung des Werkzeugs

Verwendung: `PlateSpin.VMwareRoleTool.exe /Host=Houston_Vertrieb /Benutzer=pedrom /Rolle=PlateSpinRole.xml /create`

Resultierende Aktionen:

1. Das Werkzeug für die Rollendefinition wird auf dem vCenter-Server `Houston_Vertrieb` ausgeführt, auf dem ein Administrator mit dem Benutzernamen `pedrom` vorhanden ist.
2. Wenn der Parameter `/password` nicht vorhanden ist, fordert das Werkzeug zur Eingabe des Benutzerpassworts auf, das Sie eingeben müssen.
3. Das Werkzeug greift auf die Rollendefinitionsdatei (`PlateSpinRole.xml`) zu, die sich im selben Verzeichnis befindet wie die ausführbare Datei für das Werkzeug (der Pfad dazu musste nicht näher definierte werden).
4. Das Werkzeug findet die Definitionsdatei und wird angewiesen (`/Erstellen`), die im Inhalt dieser Datei definierten Rollen in der vCenter-Umgebung zu erstellen.
5. Das Werkzeug greift auf die Definitionsdatei zu und erstellt die neuen Rollen (einschließlich der entsprechenden Mindestberechtigungen für den definierten, eingeschränkten Zugriff) innerhalb von vCenter.

   Die neuen benutzerdefinierten Rollen müssen später Benutzern in vCenter zugewiesen werden.

(Optional) Manuelle Definition der PlateSpin-Rollen in vCenter

Sie verwenden den vCenter-Client, um die benutzerdefinierten PlateSpin-Rollen zu erstellen und zuzuweisen. Dazu ist es erforderlich, die Rollen mit den aufgeführten Berechtigungen wie in `PlateSpinRole.xml` definiert zu erstellen. Wenn Sie die Rollen manuell erstellen, gibt es für den Namen der Rollen keine Beschränkungen. Die einzige Beschränkung besteht darin, dass die Rollennamen, die Sie entsprechend der Rollen in der Definitionsdatei erstellen, über alle Mindestberechtigungen verfügen, die in der Definitionsdatei aufgeführt sind.

Weitere Informationen zur Erstellung von benutzerdefinierten Rollen in vCenter finden Sie im Abschnitt *Verwalten der VMWare VirtualCenter-Rollen und -Berechtigungen* (http://www.vmware.com/pdf/vi3_vc_roles.pdf) im technischen Ressourcen-Center von VMware.

5.3.2 Zuweisen von Rollen in vCenter

Beim Einrichten einer Mehrmandantenumgebung müssen Sie pro Kunde oder „Mandant“ einen einzelnen Protect-Server bereitstellen. Sie weisen diesem Protect-Server einen aktivierten Benutzer mit bestimmten Protect-VMware-Rollen zu. Dieser aktivierte Benutzer erstellt den Protect-Container. Als Service-Anbieter bewahren Sie den Berechtigungsnachweis dieses Benutzers auf und geben ihn Ihrem Mandantenkunden nicht bekannt.

In der folgenden Tabelle sind die Rollen aufgeführt, die Sie benötigen, um den aktivierten Benutzer zu definieren. Sie enthält auch weitere Informationen über den Zweck der Rolle:

vCenter-Container für die Rollenzuweisung	Details zur Rollenzuweisung	Anweisungen für die Übertragung	Weitere Informationen
Stamm des vCenter-Inventarbaums	Weisen Sie dem aktivierten Benutzer die *PlateSpin-Infrastruktur-Manager*-Rolle (oder eine entsprechende Rolle) zu.	Aus Sicherheitsgründen müssen Sie die Berechtigung als nicht übertragbar definieren.	Diese Rolle ist erforderlich, um Aufgaben zu überwachen, die von der Protect-Software ausgeführt werden, und um abgelaufene WMware-Sitzungen zu beenden.
Alle Rechenzentrumobjekte, auf die der aktivierte Benutzer zugreifen muss	Weisen Sie dem aktivierten Benutzer die *PlateSpin-Infrastruktur-Manager*-Rolle (oder eine entsprechende Rolle) zu.	Aus Sicherheitsgründen müssen Sie die Berechtigung als nicht übertragbar definieren.	Diese Rolle ist erforderlich, um den Zugriff auf die Datenspeicher des Rechenzentrums für den Datei-Upload/Download zuzulassen. Definieren Sie die Berechtigung als nicht übertragbar.
Jeder Cluster, der als Container zu Protect hinzugefügt werden soll, und jeder Host, der im Cluster enthalten ist	Weisen Sie dem aktivierten Benutzer die *PlateSpin-Infrastruktur-Manager*-Rolle (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Für die Zuweisung zu einem Host müssen Sie die Berechtigung vom Cluster-Objekt übertragen oder eine zusätzliche Berechtigung an jedem Cluster-Host erstellen. Wenn die Rolle am Cluster-Objekt zugewiesen und übertragen wird, sind keine weiteren Änderungen beim Hinzufügen eines neuen Hosts zum Cluster erforderlich. Die Übertragung dieser Berechtigung bringt jedoch Auswirkungen auf die Sicherheit mit sich.
Jeder Ressourcen-Pool, auf den der aktivierte Benutzer zugreifen muss	Weisen Sie dem aktivierten Benutzer die Rolle des *PlateSpin-Managers für virtuelle Maschinen* (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Obwohl Sie den Zugriff auf eine beliebige Anzahl von Ressourcen-Pools an einem Standort im Baum zuweisen können, müssen Sie dem aktivierten Benutzer diese Rolle an mindestens einem Ressourcen-Pool zuweisen.

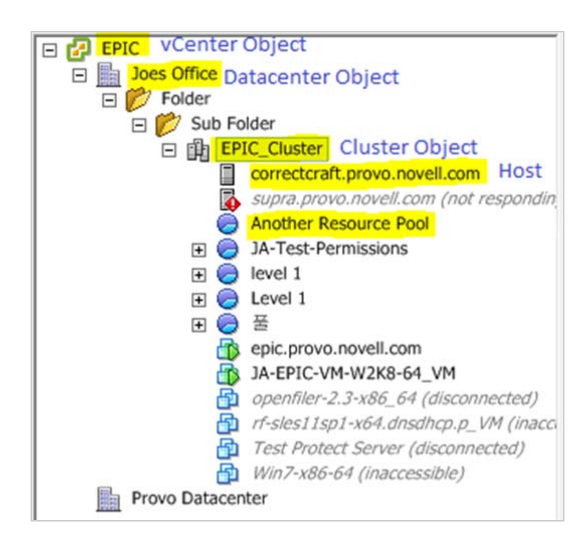
vCenter-Container für die Rollenzuweisung	Details zur Rollenzuweisung	Anweisungen für die Übertragung	Weitere Informationen
Jeder VM-Ordner, auf den der aktivierte Benutzer zugreifen muss	Weisen Sie dem aktivierten Benutzer die Rolle des *PlateSpin-Managers für virtuelle Maschinen* (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Obwohl Sie den Zugriff auf eine beliebige Anzahl von VM-Ordnern an einem beliebigen Standort im Baum zuweisen können, müssen Sie dem aktivierten Benutzer diese Rolle an mindestens einem Ordner zuweisen.
Jedes Netzwerk, auf das der aktivierte Benutzer zugreifen muss Verteilte virtuelle Netzwerke mit einem dvSwitch und einer dvPortgroup	Weisen Sie dem aktivierten Benutzer die Rolle des *PlateSpin-Managers für virtuelle Maschinen* (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Obwohl Sie den Zugriff auf eine beliebige Anzahl von Netzwerken an einem beliebigen Standort im Baum zuweisen können, müssen Sie dem aktivierten Benutzer diese Rolle an mindestens einem Ordner zuweisen. ◆ Um dem dvSwitch die richtige Rolle zuzuweisen, müssen Sie die Rolle auf das Rechenzentrum übertragen (wodurch ein weiteres Objekt erstellt wird, das die Rolle erhält) oder den dvSwitch in einen Ordner stellen und die Rolle an diesem Ordner zuweisen. ◆ Damit eine Standard-Portgruppe als verfügbares Netzwerk an der Protect-Oberfläche aufgeführt wird, müssen Sie dafür an jedem Host im Cluster eine Definition erstellen.
Jeder Datenspeicher und Datenspeicher-Cluster, auf den der aktivierte Benutzer zugreifen muss	Weisen Sie dem aktivierten Benutzer die Rolle des *PlateSpin-Managers für virtuelle Maschinen* (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Dem aktivierten Benutzer muss diese Rolle an mindestens einem Datenspeicher oder Datenspeicher-Cluster zugewiesen worden sein. Bei Datenspeicher-Clustern muss die Berechtigung an die darin enthaltenen Datenspeicher übertragen werden. Wenn für ein einzelnes Mitglied des Clusters kein Zugriff bereitgestellt wurde, treten bei vorbereiteten und vollständigen Reproduktionen Fehler auf.

In der folgenden Tabelle sehen Sie die Rolle, die Sie dem Kunden oder Mandantenbenutzer zuweisen können.

vCenter-Container für die Rollenzuweisung	Details zur Rollenzuweisung	Anweisungen für die Übertragung	Weitere Informationen
Alle Ressourcen-Pools und Ordner, in denen die virtuellen Maschinen des Kunden erstellt werden	Weisen Sie dem Mandantenbenutzer die *PlateSpin-Benutzer*-Rolle (oder eine entsprechende Rolle) zu.	Die Übertragung liegt im Ermessen des VMware-Administrators.	Dieser Mandant ist Mitglied der PlateSpin-Administratorgruppe am PlateSpin Protect-Server und ist auch am vCenter-Server vorhanden. Wenn der Mandant die von der virtuellen Maschine verwendeten Ressourcen (also die Netzwerke, ISO-Images etc.) ändern darf, müssen Sie diesem Benutzer dazu die nötigen Berechtigungen an diesen Ressourcen erteilen. Wenn Sie dem Kunden beispielsweise erlauben möchten, das Netzwerk zu ändern, in das seine virtuelle Maschine eingebunden ist, dann sollten Sie diesem Benutzer (mindestens) die schreibgeschützte Rolle (oder eine höhere Rolle) an allen Netzwerken zuweisen, auf die der Kunde zugreifen darf.

In der folgenden Abbildung ist eine virtuelle Infrastruktur in der vCenter-Konsole dargestellt. Den blau gekennzeichneten Objekten wird die Infrastruktur-Manager-Rolle zugewiesen. Den grün gekennzeichneten Objekten wird die Rolle des Managers für virtuelle Maschinen zugewiesen. Der Baum zeigt keine VM-Ordner, Netzwerke und Datenspeicher. Diesen Objekten wird die Rolle des *PlateSpin-Managers für virtuelle Maschinen* zugewiesen.

Abbildung 5-1 *In vCenter zugewiesene Rollen*



Auswirkungen auf die Sicherheit durch Zuweisen von VMware-Rollen

Die PlateSpin-Software verwendet einen aktivierten Benutzer nur zur Durchführung von Schutzmaßnahmen für Lebenszyklusvorgängen. Aus Ihrer Sicht als Service-Anbieter hat ein Endbenutzer niemals Zugriff auf den Berechtigungsnachweis des aktivierten Benutzers und kann nicht auf denselben Satz von VMware-Ressourcen zugreifen. In einer Umgebung, in der mehrere Protect-Server für die Verwendung derselben vCenter-Umgebung konfiguriert sind, verhindert Protect die Möglichkeit für den Zugriff über mehrere Clients hinweg. Die wichtigsten Auswirkungen auf die Sicherheit sind wie folgt:

- Wenn die Rolle des *PlateSpin-Infrastruktur-Managers* dem vCenter-Objekt zugewiesen wurde, kann jeder aktivierte Benutzer die von jedem anderen Benutzer ausgeführten Aufgaben sehen (doch diese nicht bearbeiten).
- Da es keine Möglichkeit gibt, Berechtigungen an Datenspeicherordnern/-unterordnern festzulegen, haben alle aktivierten Benutzer mit Berechtigungen an einem Datenspeicher Zugriff auf die Festplatten aller anderen aktivierten Benutzer, die im Datenspeicher gespeichert sind.
- Wenn die Rolle des *PlateSpin-Infrastruktur-Managers* dem Cluster-Objekt zugewiesen wurde, kann jeder aktivierte Benutzer HA oder DRS am gesamten Cluster aus- oder einschalten
- Wenn die *PlateSpin-Benutzer*-Rolle am Speicher-Cluster-Objekt zugewiesen wurde, kann jeder aktivierte Benutzer SDRS für den gesamten Cluster aus- oder einschalten
- Durch Festlegen der Rolle des *PlateSpin-Infrastruktur-Managers* am DRS-Cluster-Objekt und Übertragen dieser Rolle kann der aktivierte Benutzer alle virtuelle Maschinen sehen, die sich im Standard-Ressourcen-Pool und/oder Standard-VM-Ordner befinden. Für die Übertragung ist es außerdem erforderlich, dass der Administrator ausdrücklich für den aktivierten Benutzer festlegt, dass dieser eine „Nicht-Zugriff“-Rolle an jedem Ressourcen-Pool/VM-Ordner erhält, auf die dieser aktivierte Benutzer nicht zugreifen sollte.
- Durch Festlegen der Rolle des *PlateSpin-Infrastruktur-Managers* am vCenter-Objekt darf der aktivierte Benutzer Sitzungen von anderen Benutzern beenden, die mit dem vCenter verbunden sind.

HINWEIS: Denken Sie daran, dass in diesen Szenarien die unterschiedlichen aktivierten Benutzer tatsächlich verschiedene Instanzen der PlateSpin-Software darstellen.

5.4 Datenübertragung

In den nachfolgenden Themen finden Sie Informationen zu den Mechanismen und Optionen für die Datenübertragung aus Ihren Workloads in die entsprechenden Reproduktionen.

- Abschnitt 5.4.1, „Übertragungsmethoden“, auf Seite 83
- Abschnitt 5.4.2, „Datenverschlüsselung“, auf Seite 84

5.4.1 Übertragungsmethoden

Eine Übertragungsmethode legt fest, wie Daten eines Ursprungs-Workloads auf einem Ziel reproduziert werden. PlateSpin Protect bietet unterschiedliche Datenübertragungsmöglichkeiten, die vom Betriebssystem des geschützten Workloads abhängen.

- „Unterstützte Übertragungsmethoden für Windows-Workloads“, auf Seite 83
- „Unterstützte Übertragungsmethoden für Linux-Workloads“, auf Seite 84

Unterstützte Übertragungsmethoden für Windows-Workloads

Für Windows-Workloads bietet PlateSpin Protect verschiedene Mechanismen, mit denen Sie die Volume-Daten des Workloads entweder auf Blockebene oder auf Dateiebene übertragen.

- ❐ **Windows-Reproduktion auf Blockebene:** Daten werden auf dem Volume auf Blockebene reproduziert. Bei dieser Übertragungsmethode bietet PlateSpin Protect zwei Mechanismen, die sich durch ihre Auswirkungen auf die Kontinuität und durch ihre Leistungen unterscheiden. Sie können je nach Bedarf zwischen diesen beiden Mechanismen umschalten.
  - **Reproduktion mit der blockbasierten Komponente:** Diese Option verwendet eine blockbasierte Komponente und nutzt den Microsoft Volume Snapshot Service (VSS) mit Anwendungen und Diensten, die VSS unterstützen. Die Komponente wird dabei automatisch auf dem geschützten Workload installiert.

    HINWEIS: Für die Installation und Deinstallation der blockbasierten Komponenten ist ein Neustart des geschützten Workloads erforderlich. Wenn Windows-Cluster mit einer Datenübertragung auf Blockebene geschützt werden sollen, ist kein Neustart erforderlich. Beim Konfigurieren der Details für den Workload-Schutz können Sie wahlweise angeben, dass die Komponente erst zu einem späteren Zeitpunkt installiert werden soll, so dass der erforderliche Neustart bis zur ersten Reproduktion aufgeschoben wird.

  - **Reproduktion ohne die blockbasierte Komponente:** Diese Option verfolgt die Änderungen an den geschützten Volumes mithilfe eines internen „Hashing“-Mechanismus in Kombination mit Microsoft VSS.

    Diese Option erfordert keinen Neustart, bietet jedoch niedrigere Leistungen als die blockbasierte Komponente.
- ❐ **Windows-Reproduktion auf Dateiebene:** Die Daten werden dateiweise reproduziert (nur Windows).

Unterstützte Übertragungsmethoden für Linux-Workloads

Für Linux-Workloads bietet PlateSpin Protect einen Mechanismus, mit dem Sie die Volume-Daten des Workloads ausschließlich auf Blockebene übertragen. Die Datenübertragung wird mithilfe einer Datenübertragungskomponente auf Blockebene durchgeführt, die LVM-Snapshots nutzt, sofern vorhanden (die standardmäßige und empfohlene Option). Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7005872.

Die im Lieferumfang von PlateSpin Protect enthaltene blockbasierte Linux-Komponente ist für Standard- und Nicht-Debug-Kernels der unterstützen Linux-Distributionen vorkompiliert. Wenn Sie einen nicht-standardmäßigen, benutzerdefinierten oder neueren Kernel haben, können Sie die blockbasierte Komponente gemäß den Spezifikationen Ihres Kernels neu aufbauen. Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7005873.

Das Bereitstellen bzw. Entfernen der Komponente wird im Hintergrund ausgeführt, beeinträchtigt nicht die Kontinuität und erfordert keinen Benutzereingriff und Neustart.

5.4.2 Datenverschlüsselung

PlateSpin Protect ermöglicht Ihnen, die Datenreproduktion zu verschlüsseln, um die Übertragung Ihrer Workload-Daten sicherer zu machen. Wenn die Verschlüsselung aktiviert ist, wird die Datenübertragung im Netz vom Ursprung zum Ziel über AES (Advanced Encryption Standard) oder 3DES verschlüsselt, falls die FIPS-kompatible Verschlüsselung aktiviert ist. (Weitere Informationen finden Sie unter „Aktivieren der Unterstützung für FIPS-kompatible Datenverschlüsselungsalgorithmen (optional)“ im *PlateSpin Protect Installations- und Aufrüstungshandbuch*.)

HINWEIS: Die Verschlüsselung wirkt sich auf die Leistung aus und kann die Datenübertragungsgeschwindigkeit erheblich beeinträchtigen.

5.5 Schutzebenen

Bei einer Schutzebene handelt es sich um eine benutzerdefinierbare Sammlung von Workload-Schutz-Parametern, die Folgendes definieren:

- Die Häufigkeit und das Wiederholungsmuster von Reproduktionen
- Ob die Datenübertragung verschlüsselt werden soll
- Ob und wie eine Datenkomprimierung durchgeführt werden soll
- Ob die verfügbare Bandbreite während des Datentransfers auf eine bestimmte Durchsatzrate gedrosselt werden soll
- Kriterien, anhand deren das System einen Workload als offline (fehlgeschlagen) erachtet

Eine Schutzebene ist ein wesentlicher Bestandteil jedes Workload-Schutzvertrages. In der Konfigurationsphase eines Workload-Schutzvertrages können Sie eine von mehreren integrierten Schutzebenen auswählen und ihre Attribute entsprechend den Anforderungen des spezifischen Schutzvertrages anpassen.

Sie können benutzerdefinierte Schutzebenen auch vorab erstellen:

1. Klicken Sie auf Ihrer PlateSpin Protect-Weboberfläche auf **Einstellungen > Schutzebenen > Schutzebene erstellen**.
2. Geben Sie die Parameter für die neue Schutzebene ein:

Name	Geben Sie einen Namen für die Ebene ein.
Inkrementelle Wiederholung	Geben Sie die Häufigkeit der inkrementellen Reproduktionen und das inkrementelle Wiederholungsmuster an. Sie können das Datum direkt in das Feld **Beginn der Wiederholung** eingeben oder auf das Kalendersymbol klicken, um ein Datum auszuwählen. Wählen Sie **Keine** als Wiederholungsmuster, wenn nie eine inkrementelle Reproduktion ausgeführt werden soll.
Vollständige Wiederholung	Geben Sie die Häufigkeit der Vollreproduktionen und das Muster der vollständigen Wiederholung an.
Sperrzeit	Verwenden Sie diese Einstellungen, um eine Wiederherstellungs-Sperrzeit durchzusetzen (um geplante Wiederherstellungen bei Spitzenauslastungszeiten auszusetzen oder um Konflikte zwischen VSS-bewusster Software und der PlateSpin-Komponente für den VSS-Datentransfer auf Blockebene zu vermeiden). Klicken Sie zum Festlegen einer Sperrzeit auf **Bearbeiten** und wählen Sie ein Wiederholungsmuster (Täglich, Wöchentlich etc.) sowie die Anfangs- und Endzeit der Sperrzeit. **HINWEIS:** Die Anfangs- und Endzeiten für die Sperrzeit hängen von der Systemuhr an Ihrem PlateSpin-Server ab.
Komprimierungsgrad	Diese Einstellungen legen fest, ob und wie Workload-Daten vor der Übertragung komprimiert werden. Weitere Informationen hierzu finden Sie in „Datenkomprimierung“, auf Seite 20. Wählen Sie eine der verfügbaren Optionen aus. **Schnell** verbraucht die wenigsten CPU-Ressourcen auf dem Ursprung, geht jedoch mit einer geringeren Komprimierung einher. **Maximal** verbraucht die meisten Ressourcen, erzielt aber auch eine höhere Komprimierung. **Optimal** liegt dazwischen und ist die empfohlene Option.
Bandbreitendrosselung	Diese Einstellungen steuern die Bandbreitendrosselung. Weitere Informationen hierzu finden Sie in „Bandbreitendrosselung“, auf Seite 20. Um die Bandbreite bei Reproduktionen auf eine bestimmte Rate zu drosseln, geben Sie den erforderlichen Durchsatzwert in Mb/s sowie das Zeitmuster ein.
Beizubehaltende Wiederherstellungspunkte	Geben Sie die Anzahl der beizubehaltenden Wiederherstellungspunkte für Workloads an, die diese Schutzebene verwenden. Weitere Informationen hierzu finden Sie unter „Wiederherstellungspunkte“, auf Seite 86.
Workload-Fehler	Geben Sie an, wie viele Versuche zur Workload-Erkennung durchgeführt werden sollen, bis der Workload als fehlgeschlagen erachtet wird.
Workload-Erkennung	Geben Sie das Zeitintervall (in Sekunden) zwischen den Workload-Erkennungsversuchen an.

5.6 Wiederherstellungspunkte

Ein Wiederherstellungspunkt ist ein zu einem bestimmten Zeitpunkt erstellter Snapshot eines Workloads. Er ermöglicht es, einen reproduzierten Workload in einem bestimmten Zustand wiederherzustellen.

Jeder geschützte Workload verfügt über mindestens einen und höchstens 32 Wiederherstellungspunkte.

WARNUNG: Wiederherstellungspunkte, die sich im Laufe der Zeit anhäufen, können dazu führen, dass der Speicherplatz von PlateSpin Protect nicht mehr ausreicht.

5.7 Anfängliche Reproduktionsmethode (vollständig und inkrementell)

Bei Workload-Schutz- und Failback-Vorgängen bestimmt der Parameter „Anfängliche Reproduktion“ den Umfang der Daten, die von einem Ursprung auf ein Ziel übertragen werden.

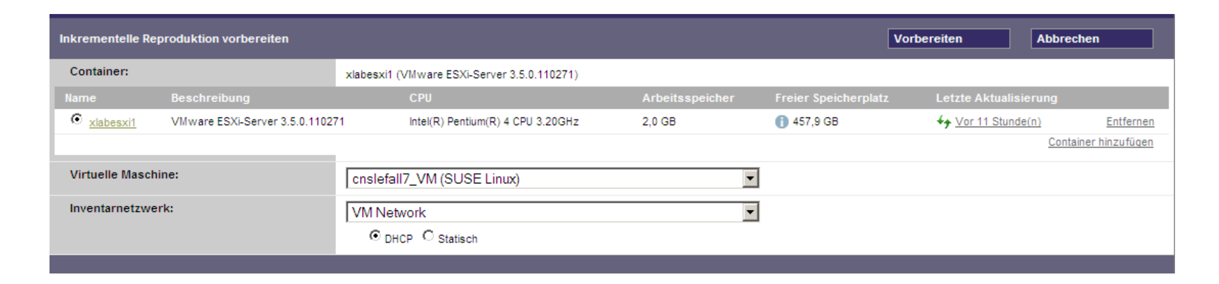
- **Vollständig:** Eine vollständige Volume-Übertragung erfolgt von einem Produktions-Workload auf dessen Reproduktion (der Failover-Workload) oder von einem Failover-Workload auf seine ursprüngliche virtuelle oder physische Infrastruktur.
- **Inkrementell:** Es werden nur Unterschiede vom Ursprung auf dessen Ziel übertragen, vorausgesetzt, sie verfügen über ähnliche Betriebssysteme und Volume-Profile.
  - Beim Schutz: Der Produktions-Workload wird mit einer vorhandenen VM im VM-Container verglichen. Bei der vorhandenen VM kann es sich um eine der folgenden VMs handeln:
    - Die Wiederherstellungs-VM eines bereits geschützten Workloads (wenn die Option **VM löschen** des Befehls **Workload entfernen** deaktiviert wurde).
    - Ein virtueller Computer (VM), der manuell in den VM-Container importiert wurde, wie z. B. ein Workload-VM, der auf einem Wechseldatenträger physisch vom Produktionsstandort auf einen Remote-Wiederherstellungsstandort verschoben wird.

      Weitere Informationen hierzu finden Sie in der VMware-Dokumentation.
  - Während des Failbacks auf eine virtuelle Maschine wird der Failover-Workload mit einer vorhandenen VM in einem Failback-Container verglichen.
  - Während des Failbacks auf einen physischen Computer wird der Failover-Workload mit einem Workload auf der physischen Zielmaschine verglichen, sofern der physische Computer bei PlateSpin Protect registriert ist (siehe „Halbautomatischer Failback auf einen physischen Computer“, auf Seite 71).

Wenn Sie während des Workload-Schutzes und Failbacks auf einen VM-Host **Inkrementell** als anfängliche Reproduktionsmethode wählen, müssen Sie zur Ziel-VM navigieren und diese für eine Synchronisierung mit dem Ursprung des ausgewählten Vorgangs vorbereiten.

1. Fahren Sie mit dem erforderlichen Workload-Befehl fort, z. B. **Konfigurieren (Schutzdetails)** oder **Failback**.
2. Wählen Sie für **Anfängliche Reproduktionsmethode** die Option **Inkrementelle Reproduktion**.
3. Klicken Sie auf **Workload vorbereiten**.

   Auf der PlateSpin Protect-Weboberfläche wird die Seite „Inkrementelle Reproduktion vorbereiten“ angezeigt.



4 Wählen Sie den erforderlichen Container, die virtuelle Maschine und das Inventarnetzwerk aus, das für die Kommunikation mit der VM verwendet werden soll. Wenn der angegebene Zielcontainer ein VMware DRS-Cluster ist, können Sie außerdem einen Ziel-Ressourcenpool angeben, dem das System den Workload zuweisen soll.

5 Klicken Sie auf **Vorbereiten**.

   Warten Sie, bis der Prozess abgeschlossen wurde und darauf, dass die Benutzerschnittstelle zum ursprünglichen Befehl zurückkehrt, und wählen Sie den vorbereiteten Workload aus.

HINWEIS: (Nur Datenreproduktionen auf Blockebene) Die erste inkrementelle Reproduktion dauert deutlich länger als nachfolgende Reproduktionen. Dies liegt daran, dass das System die Volumes auf dem Ursprung und dem Ziel Block für Block miteinander vergleichen muss. Alle nachfolgenden Reproduktionen verlassen sich auf die Änderungen, die bei der Ausführung eines aktiven Workloads von der blockbasierten Komponente erkannt wurden.

5.8 Steuerung von Diensten und Daemons

PlateSpin Protect ermöglicht Ihnen die Steuerung von Diensten und Daemons:

- **Steuerung des Diensts/Daemons:** Während des Datentransfers können Sie Windows-Dienste oder Linux-Daemons, die auf dem Ursprungs-Workload ausgeführt werden, automatisch anhalten. Dadurch wird sichergestellt, dass der Workload in einem stabileren Zustand reproduziert wird als wenn er weiterhin ausgeführt werden würden.

  Beispielsweise sollten Sie bei Windows-Workloads Dienste von Virenschutz-Software oder von VSS-Backup-Software anderer Hersteller anhalten.

  Um mehr Kontrolle über die Linux-Ursprünge während der Reproduktion zu haben, können Sie während jeder Reproduktion benutzerdefinierte Skripte über Ihre Linux-Workloads ausführen. Weitere Informationen hierzu finden Sie unter „Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)“, auf Seite 88.

- **Steuerung des Startstatus/der Ausführungsebene des Ziels:** Sie können den Startstatus (Windows) oder die Ausführungsebene (Linux) von Diensten/Daemons auf dem virtuellen Failover-Computer auswählen. Wenn Sie einen Failover-Vorgang oder einen Failover-Testvorgang ausführen, können Sie angeben, welche Dienste oder Daemons ausgeführt oder gestoppt werden sollen, wenn der Failover-Workload in den Live-Modus wechselt.

  Zu den allgemeinen Diensten, denen Sie den Startstatus `Deaktiviert` zuweisen sollten, gehören herstellerspezifische Dienste, die an die ihnen zugrunde liegende physische Infrastruktur gebunden und in einer virtuellen Maschine nicht erforderlich sind.

5.9 Verwenden von Freeze- und Thaw-Skripts für alle Reproduktionen (Linux)

Bei Linux-Systemen bietet PlateSpin Protect die Möglichkeit, die benutzerdefinierten Skripts `freeze` und `thaw` automatisch auszuführen. Diese Skripts ergänzen die automatische Daemon-Steuerungsfunktion.

Das Skript `freeze` wird zu Beginn einer Reproduktion ausgeführt, das Skript `thaw` am Ende.

Sie sollten diese Funktion in Ergänzung der automatisierten Daemon-Steuerungsfunktion verwenden, die über die Benutzeroberfläche zur Verfügung steht (siehe „Steuerung des Diensts/ Daemons:“, auf Seite 87). Beispielsweise können Sie diese Funktion verwenden, um bestimmte Daemons während der Reproduktion temporär anzuhalten, statt sie herunterzufahren.

Führen Sie zur Implementierung der Funktion folgende Schritte aus, bevor Sie den Linux-Workload-Schutz einrichten:

1. Erstellen Sie die folgenden Dateien:
   - `platespin.freeze.sh`: Ein zu Beginn einer Reproduktion auszuführendes Shell-Skript
   - `platespin.thaw.sh`: Ein zum Abschluss einer Reproduktion auszuführendes Shell-Skript
   - `platespin.conf`: Eine Textdatei, die alle erforderlichen Argumente sowie einen Zeitüberschreitungswert definiert.

     Der Inhalt der Datei `platespin.conf` muss in folgender Syntax angegeben werden:

     ```
     [ServiceControl]
     FreezeArguments=<Argumente>
     ThawArguments=<Argumente>
     TimeOut=<Zeitüberschreitung>
     ```

     Ersetzen Sie *<Argumente>* durch die erforderlichen Befehlsargumente, getrennt durch ein Leerzeichen, und *<Zeitüberschreitung>* durch einen Zeitüberschreitungswert in Sekunden. Wenn kein Wert angegeben wurde, wird die Standard-Zeitüberschreitung (60 Sekunden) verwendet.
2. Speichern Sie die Skripte sowie die `.conf`-Datei auf dem Linux-Ursprungs-Workload in folgendem Verzeichnis:

   `/etc/platespin`

5.10 Volumes

Beim Hinzufügen eines Workloads für den Schutz inventarisiert PlateSpin Protect die Speichermedien Ihres Ursprungs-Workloads und richtet automatisch Optionen auf der PlateSpin Protect-Weboberfläche ein, über die Sie die für den Schutz benötigten Volumes angeben können.

PlateSpin Protect unterstützt mehrere Speichertypen, darunter dynamische Windows-Datenträger, LVM (nur Version 2), RAID und SAN.

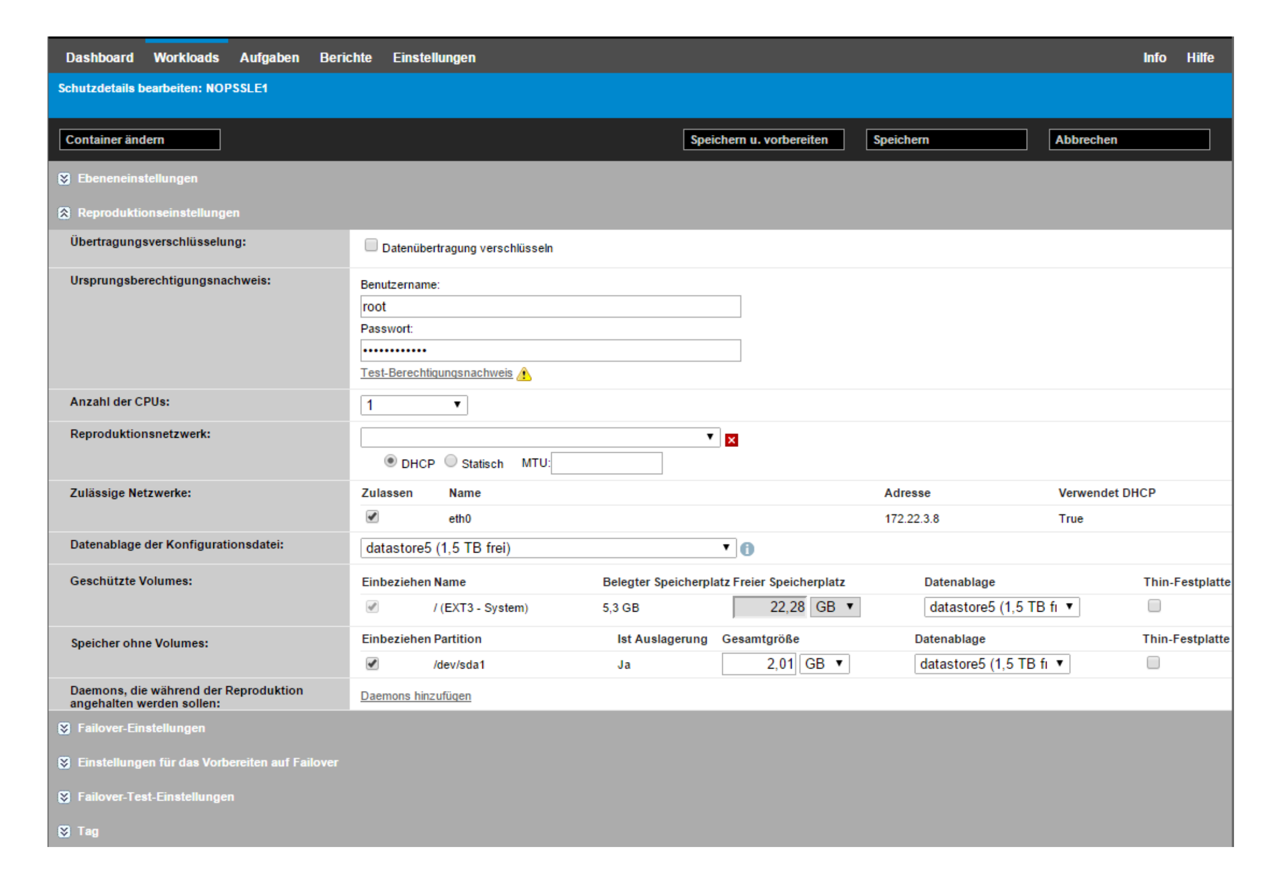
Bei Linux-Workloads bietet PlateSpin Protect folgende zusätzlichen Funktionen:

- Nicht-Volume-Speicher wie eine Swap-Partition, die mit dem Ursprungs-Workload verknüpft ist, werden im Failover-Workload neu erstellt.

* Das Layout der Volume-Gruppen und logischen Volumes wird beibehalten, sodass Sie es während des Failbacks neu erstellen können.
* (OES 2-Workloads) EVMS-Layouts von Ursprungs-Workloads werden beibehalten und im VM-Container neu erstellt. NSS-Pools werden vom Ursprung in die Wiederherstellungs-VM kopiert.

Die folgenden Abbildungen zeigen die unter „Reproduktionseinstellungen“ festgelegten Parameter für einen Linux-Workload mit mehreren Volumes und zwei logischen Volumes in einer Volume-Gruppe.

Abbildung 5-2 *Volumes, logische Volumes und Volume-Gruppen eines geschützten Linux-Workloads*



Die folgende Abbildung zeigt Volume-Schutz-Optionen eines OES 2-Workloads mit Optionen, die angeben, dass das EVMS-Layout beibehalten und für den Failover-Workload neu erstellt werden soll:

Abbildung 5-3 *Reproduktionseinstellungen, Volume-bezogene Optionen (OES 2-Workload)*

Geschützte logische Volumes:	Einbeziehen	Name	Verwendeter Speicherplatz	Freier Speicherplatz	Volume-Gruppe / EVMS-Volumes
	☑	/ (REISERFS)	2,2 GB	2,2 GB	system
	☑	/boot (EXT2)	13,0 MB	55,3 MB	/dev/evms/sda1
	☑	/opt/novell/nss/mnt/.pools/NEWPOOL (NSSFS)	23,3 MB	999,6 MB	NEWPOOL

Speicher ohne Volumes:	Einbeziehen	Partition	Ist Auslagerung	Gesamtgröße	Datenablage-/Volume-Gruppe
	☑	/dev/system/swap	Ja	1,48 GB	system

Volume-Gruppen:	Einbeziehen	Name	Gesamtgröße	Datenablage	Thin-Festplatte
	☑	system	5,9 GB	dev-comp124:storage	☐

EVMS-Volumes	Einbeziehen	Name	Ist Auslagerung	Gesamtgröße	Datenablage	Thin-Festplatte
	☑	/dev/evms/sda1		70,6 MB	dev-comp124:storage	☐
	☑	NEWPOOL		1023,0 MB	dev-comp124:storage	☐

Daemons, die während der Reproduktion angehalten werden sollen:	Daemons hinzufügen

5.11 Netzwerke

PlateSpin Protect ermöglicht Ihnen die Steuerung der Netzwerkidentität Ihres Failover-Workloads und der LAN-Einstellungen, sodass Sie verhindern können, dass der Reproduktionsdatenverkehr den LAN- oder WAN-Datenverkehr beeinträchtigt.

Sie können spezifische Netzwerkeinstellungen in den Details für den Workload-Schutz festlegen, die in unterschiedlichen Phasen des Workload-Schutz- und -Wiederherstellungs-Workflows verwendet werden:

- **Reproduktion:** (Reproduktion-Parameter festgelegt) Zur Trennung des regulären Reproduktionsdatenverkehrs vom Produktionsdatenverkehr.
- **Failover:** (Failover-Parameter festgelegt) Definiert, dass der Failover-Workload beim Wechsel in den Live-Modus Teil des Produktionsnetzwerks wird.
- **Vorbereiten auf Failover:** (Vorbereiten auf Failover-Netzwerkparameter) Für Netzwerkeinstellungen während der optionalen Failover-Vorbereitungsphase.
- **Failover testen:** (Failover testen-Parameter festgelegt) Definiert, dass Netzwerkeinstellungen während einer Failover-Testphase für den Failover-Workload gelten.

5.12 Failback auf physische Computer

Wenn die erforderliche Zielinfrastruktur für einen Failback-Vorgang ein physischer Computer ist, müssen Sie ihn in PlateSpin Protect registrieren.

Die Registrierung eines physischen Computers erfolgt durch das Booten des physischen Zielcomputers mit dem PlateSpin-Boot-Image (ISO-Image).

- Abschnitt 5.12.1, „Herunterladen des PlateSpin-Boot-ISO-Image“, auf Seite 91
- Abschnitt 5.12.2, „Einfügen weiterer Gerätetreiber in das Boot-ISO-Image“, auf Seite 91
- Abschnitt 5.12.3, „Registrieren von physischen Computern als Failback-Ziel mit PlateSpin Protect“, auf Seite 92

5.12.1 Herunterladen des PlateSpin-Boot-ISO-Image

Sie können die PlateSpin-Boot-ISO-Images (`p.iso` für BIOS-Firmware-basierte Ziele und bootofx.x2 für UEFI-Firmware-basierte Ziele) im Bereich PlateSpin Protect von Novell Downloads (http://download.novell.com) herunterladen. Führen Sie dazu eine Suche mit folgenden Parametern aus:

- **Produkt oder Technologie:** `PlateSpin Protect`
- **Version auswählen:** `PlateSpin Protect11.1`
- **Datumsbereich:** `Alle Datumsangaben`

5.12.2 Einfügen weiterer Gerätetreiber in das Boot-ISO-Image

Sie können mithilfe eines benutzerdefinierten Dienstprogramms weitere Linux-Gerätetreiber zu einem Paket zusammenstellen und in das PlateSpin-Boot-Image einfügen, bevor Sie es auf eine CD brennen:

1. Beschaffen oder kompilieren Sie geeignete `*.ko`-Treiberdateien für den Zielhardware-Hersteller.

   WICHTIG: Stellen Sie sicher, dass die Treiber mit dem in der ISO-Datei enthaltenen Kernel kompatibel sind (für x86-Systeme: `3.0.93-0.8-pae`, für x64-Systeme: `3.0.93-0.8-default`) und zur Architektur des Zielcomputers passen. Weitere Informationen finden Sie im Wissensdatenbankartikel 7005990.

2. Mounten Sie das Image in einem Linux-Computer (`root`-Berechtigungsnachweis erforderlich). Verwenden Sie die folgende Befehlssyntax:

   ```
   mount -o loop <Pfad-zu-ISO> <Mount-Punkt>
   ```

3. Kopieren Sie das Skript `rebuildiso.sh`, das sich im Unterverzeichnis `/tools` der gemounteten ISO-Datei befindet, in ein temporäres Arbeitsverzeichnis. Wenn Sie fertig sind, entladen Sie die ISO-Datei. (Führen Sie dazu den Befehl `unmount <Mount-Punkt>` aus.)

4. Erstellen Sie ein weiteres Arbeitsverzeichnis für die erforderlichen Treiberdateien und speichern Sie diese in diesem Verzeichnis.

5. Führen Sie im Verzeichnis, in dem Sie das Skript `rebuildiso.sh` gespeichert haben, das Skript `rebuildiso.sh` als `Stamm` aus und verwenden Sie dazu die folgende Syntax:

   ```
   ./rebuildiso.sh <ARGS> [-v] -m32|-m64 -i <ISO-Datei>
   ```

   In der folgenden Tabelle sind die möglichen Befehlszeilenoptionen für diesen Befehl aufgeführt:

Option	Beschreibung
`-i <ISO-Datei>`	<*ISO-Datei*> ist die ISO zum Bearbeiten, Auflisten etc.
`-v`	Falls dieser Befehl zusammen mit dem Argument `-l` verwendet wird, wird mit dieser Option der Befehl „modinfo“ zum Abrufen umfassender Treiberinformationen ausgelöst.
`-o`	Falls dieser Befehl zusammen mit dem Argument `-c` oder dem Argument `-d` verwendet wird, dann wird die alte Kopie der ISO-Datei nicht überschrieben.
`-m32`	gibt an, dass die 32-Bit-initrd einbezogen wird
`-m64`	gibt an, dass die 64-Bit-initrd einbezogen wird

In der nächsten Tabelle sind die möglichen Argumente für die Verwendung mit diesem Befehl aufgeführt. Mindestens eines dieser Argumente muss im Befehl verwendet werden:

<table>
<tr><th>Argument</th><th>Beschreibung</th></tr>
<tr><td>-d <<i>Pfad</i>></td><td><<i>Pfad</i>> gibt das Verzeichnis mit den Treibern an (d. h. *.ko-Dateien), die Sie einbeziehen möchten.

Bei Anwendung dieses Befehls wird die ISO-Datei mit den hinzugefügten Treibern aktualisiert.</td></tr>
<tr><td>-c <<i>Pfad</i>></td><td><<i>Pfad</i>> gibt an, wo sich eine ConfigureTakeControl.xml-Datei befindet.</td></tr>
<tr><td>-l [<<i>Typ</i>>]</td><td><<i>Typ</i>> gibt eine Teilmenge von Treibern an, die Sie auflisten möchten. Standardmäßig ist „alle“ Typen festgelegt.

Aufgeführte Treibertypen, die mit einem Schrägstrich (/) beginnen, befinden sich vermutlich unter <<i>Kernel-Modul-Verzeichnis</i>>/Kernel/

Aufgeführte Treibertypen, die nicht mit einem Schrägstrich (/) beginnen, befinden sich vermutlich unter <<i>Kernel-Modul-Verzeichnis</i>/Kernel/Treiber/

Beispiele für Treiber-Teilmengen:

-l scsi
-l 'net|video'
-l '/net|net'

Besondere Verwendung dieses Arguments:

Wenn Sie die verfügbaren Unterverzeichnisse der einzelnen Teilmengen aufführen möchten, verwenden Sie das Argument wie folgt: -l INDEX</td></tr>
</table>

Syntax-Beispiele

- So listen Sie einen Index von 32-Bit-Treibern auf:

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m32 -l INDEX
```

- So listen Sie Treiber auf, die im Ordner „/Verschiedene“ gefunden werden:

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m32 -l misc
```

- So beziehen Sie 32-Bit-Treiber vom Ordner „/OEM-Treiber“ ein:

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m32 -d oem-drivers
```

- So beziehen Sie 64-Bit-Treiber vom Ordner „/OEM-Treiber“ sowie eine benutzerdefinierte Datei „ConfigureTakeControl.xml“ ein:

```
# ./rebuildiso.sh -i bootofx.x2p.iso -m64 -c ConfigureTakeControl.xml -d
oem-drivers
```

5.12.3 Registrieren von physischen Computern als Failback-Ziel mit PlateSpin Protect

1. Brennen Sie das PlateSpin-Boot-ISO-Image auf eine CD oder speichern Sie es auf einem Medium, von dem Ihr Ziel booten kann.
2. Stellen Sie sicher, dass der Netzwerk-Switch-Anschluss, der mit dem Ziel verbunden ist, auf **Autom. Vollduplex** eingestellt ist.

3. Verwenden Sie die Boot-CD zum Booten des physischen Zielcomputers und warten Sie, bis das Befehlszeilenfenster geöffnet wird.
4. (Nur Linux) Geben Sie bei 64-Bit-Systemen im anfänglichen Bootprompt Folgendes ein:
   - `ps64` (für Systeme mit bis zu 512 MB RAM)
   - `ps64_512m` (für Systeme mit mehr als 512 MB RAM)
5. Drücken Sie die Eingabetaste.
6. Geben Sie nach der Eingabeaufforderung den Hostnamen oder die IP-Adresse Ihres PlateSpin-Server-Hosts ein.
7. Geben Sie den Administrator-Berechtigungsnachweis für den PlateSpin Server-Host einschließlich einer Zertifizierungsstelle an. Verwenden Sie für das Benutzerkonto das folgende Format:

   Domäne\Benutzername oder *Hostname\Benutzername*

   Verfügbare Netzwerkkarten werden anhand ihrer MAC-Adressen erkannt und angezeigt.
8. Wenn DHCP auf der zu verwendenden NIC verfügbar ist, drücken Sie die Eingabetaste, um fortzufahren. Wenn DHCP nicht verfügbar ist, geben Sie an, dass die erforderliche NIC mit einer statischen IP-Adresse konfiguriert werden soll.
9. Geben Sie einen Hostnamen für den physischen Computer ein oder drücken Sie die Eingabetaste, um die Standardwerte zu übernehmen.
10. Wenn Sie dazu aufgefordert werden, anzugeben, ob Sie HTTPS verwenden möchten, müssen Sie `J` eingeben, wenn Sie SSL aktiviert haben, oder `N`, wenn dies nicht der Fall ist.

Nach kurzer Zeit sollte der physische Computer in den Failback-Einstellungen der PlateSpin Protect-Weboberfläche verfügbar sein.

5.13 Themen zu erweitertem Workload-Schutz

5.13.1 Schützen von Windows-Clustern

PlateSpin Protect unterstützt den Schutz der Geschäftsdienste eines Microsoft Windows-Clusters. Folgende Cluster-Technologien werden unterstützt:

- Windows 2008 R2 Server-basiertes Microsoft-Failovercluster

Dieser Abschnitt enthält folgende Informationen:

HINWEIS: Weitere Informationen zum Neuaufbauen der Windows 2008/2008R2-Failover-Cluster-Umgebung nach erfolgtem Schutz durch PlateSpin Protect beim Failover/Failback finden Sie im Wissensdatenbankartikel 7015576.

Workload-Schutz

Der Schutz eines Clusters wird durch inkrementelle Reproduktionen der Änderungen auf dem aktiven Knoten erreicht, die an einen virtuellen Einzelknoten-Cluster übertragen werden, den Sie während der Fehlerbehebung an der Ursprungsinfrastruktur verwenden können.

Der Umfang der Unterstützung von Cluster-Migrationen in der aktuellen Version ist von folgenden Bedingungen abhängig:

- Wenn Sie einen Vorgang des Typs **Workload hinzufügen** durchführen, müssen Sie über die IP-Adresse des Clusters (*Virtuelle IP-Adresse*) den aktiven Knoten identifizieren, d. h. den Knoten, der zurzeit die Quorum-Ressource des Clusters besitzt. Wenn Sie die IP-Adresse eines einzelnen Knotens angeben, wird dieser Knoten als regulärer Windows-Workload inventarisiert (das Cluster bleibt unerkannt).
- Eine Quorum-Ressource eines Clusters muss zu der Ressourcengruppe (Dienst) des Clusters gehören, die geschützt wird.

Bei einer blockbasierten Übertragung werden die blockbasierten Treiberkomponenten nicht auf dem Clusterknoten installiert. Die blockbasierte Übertragung erfolgt anhand einer treiberlosen Synchronisierung mit einer MD5-basierten Reproduktion. Da der blockbasierte Treiber nicht installiert ist, ist kein Neustart auf den Clusterknoten der Quelle erforderlich.

HINWEIS: Die dateibasierte Übertragung wird nicht unterstützt, um die Microsoft Windows-Cluster zu schützen.

Wenn ein Knoten-Failover zwischen inkrementellen Reproduktionen eines geschützten Clusters auftritt und das neue Profil des aktiven Knotens in etwa dem fehlerhaften aktiven Knoten entspricht, wird der Schutzvertrag wie geplant fortgesetzt; andernfalls wird der Befehl nicht ausgeführt. Die Profile der Clusterknoten werden als ähnlich erachtet, wenn:

- sie dieselbe Anzahl an Volumes haben.
- alle Volumes auf allen Knoten exakt dieselbe Größe haben.
- sie eine identische Anzahl an Netzwerkverbindungen haben.
- Seriennummern für lokale Volumes (System-Volume und Reserviertes System-Volume) müssen auf allen Clusterknoten gleich sein.

  Wenn die lokalen Treiber auf allen Knoten des Clusters verschiedene Seriennummern aufweisen, können Sie keine inkrementelle Reproduktion ausführen, nachdem der aktive Knoten im Falle eines Knotenfehlers wechselt. Beispiel: Der aktive Knoten ist Knoten 1 und er „wechselt“ zu Knoten 2.

  Für Protect 11.1 stehen zwei unterstützte Optionen zur Unterstützung von Clustern in diesem Szenario zur Verfügung:

  - (Empfohlen) Verwenden Sie das angepasste Dienstprogramm *Volume Manager*, um die Seriennummern des lokalen Volumes zu ändern, damit sie mit den einzelnen Knoten des Clusters übereinstimmen. Weitere Informationen finden Sie unter Anhang B, „Synchronisieren von Seriennummern im lokalen Clusterknoten-Speicher“, auf Seite 127.
  - (Bedingt und optional) Wenn Sie den folgenden Fehler sehen:

    ```
    Volume mappings does not contain source serial number: xxxx-xxxx,
    ```

    Er wurde möglicherweise durch eine Änderung im aktiven Knoten vor Ausführung der inkrementellen Reproduktion verursacht. In diesem Fall können Sie eine vollständige Reproduktion ausführen, um sicherzustellen, dass der Cluster wieder geschützt ist. Inkrementelle Reproduktionen sollten nach der vollständigen Reproduktion wieder funktionieren.

Wenn die Volume-Seriennummern nicht mit den einzelnen Knoten im Cluster übereinstimmen sollen, ist vor jeder inkrementellen Reproduktion eine vollständige Reproduktion erforderlich, sobald der aktive Knoten ein Failover auf einen neuen Knoten im Cluster durchführt.

Wenn während einer vollständigen oder inkrementellen Reproduktion ein Knoten-Failover vor Abschluss des Kopiervorgangs auftritt, dann wird der Befehl abgebrochen und eine Meldung wird angezeigt, die besagt, dass die Reproduktion erneut ausgeführt werden muss.

Um ein Windows-Cluster zu schützen, gehen Sie nach dem gleichen Ablaufplan wie für den normalen Workload-Schutz vor (siehe „Grundlegender Workflow für den Workload-Schutz und die Wiederherstellung“, auf Seite 57).

Schutz-Failover

Wenn der Failover-Vorgang abgeschlossen ist und der Failover-Computer online geht, sehen Sie ein Cluster mit mehreren Knoten, bei dem ein Knoten aktiv ist (alle anderen Knoten sind nicht verfügbar).

Für ein Failover (oder ein Test-Failover) auf einem Windows-Cluster muss das Cluster eine Verbindung zu einem Domänencontroller herstellen können. Zur Nutzung der Test-Failover-Funktion müssen Sie den Domänencontroller zusammen mit dem Cluster schützen. Während des Tests müssen Sie den Domänencontroller hochfahren, gefolgt vom Windows-Cluster-Workload (in einem isolierten Netzwerk).

Schutz-Failback

Für diese Version wird nur ein Failback unterstützt, das die vollständige Reproduktion für Windows Cluster-Arbeitsauslastungen verwendet.

Wenn Sie das Failback als vollständige Reproduktion auf ein physisches Ziel konfigurieren, können Sie eine der folgenden Methoden verwenden:

- Ordnen Sie alle Festplatten auf dem Failover-Rechner einer einzigen lokalen Festplatte auf dem Failback-Ziel zu.
- Fügen Sie dem physischen Failback-Rechner eine andere Festplatte `Festplatte 2`) hinzu. Sie können den Failback-Vorgang dann konfigurieren, um das System-Volume des Failovers auf `Festplatte 1` und die zusätzlichen Festplatten des Failovers (zuvor gemeinsam genutzte Festplatten) auf `Festplatte 2` wiederherzustellen. So kann die Systemfestplatte auf die Speicherfestplatte mit gleicher Größe wiederhergestellt werden wie die ursprüngliche Quelle.

Nach Abschluss des Failbacks können Sie andere Knoten mit dem erneut reproduzierten Cluster zusammenführen.

5.13.2 Verwenden von Workload-Schutz-Funktionen über die PlateSpin Protect-Web-Services-API

Mithilfe der `protectionservices`-API können Sie Workload-Schutz-Funktionen programmatisch von Ihren Anwendungen aus verwenden. Alle Programmier- oder Skriptsprachen, die einen HTTP-Client und das JSON-Serialisierungs-Framework nutzen, sind verwendbar.

`https://`*<hostname | IP-Adresse>*/`protectionservices`

Ersetzen Sie *<Hostname | IP-Adresse>* durch den Hostnamen oder die IP-Adresse Ihres PlateSpin Server-Hosts. Wenn SSL nicht aktiviert ist, verwenden Sie `http` in der URL.

Abbildung 5-4 Die erste Seite der API des Serverschutzes

PlateSpin Protect Server API

Version 4.0.0.1161

Documentation

Getting started

- Getting started with API
- Security and authentication
- Developer Guidelines
- Troubleshooting
- FAQ

How to

- Steps to protect workload
- Working with workload
- Working with container
- Working with security groups
- Working with protection tiers
- Limitations of the API
- Samples
- Glossary

REST Resources (auto-generated)

- Containers
- Workloads
- Configuration
- Operations
- Protection Tiers
- Security Groups

Resource representations

This section specifies the representations of the resources which this API operates on. The representations are made up of fields, each with a name and value, encoded using a JSON dictionary. The values may be numeric or string literals, lists, or dictionaries, each of which are represented in the obvious way in JSON. These representations typically nest. For example, the representation of a Containers will include representations of the Container which inhabit it, which in turn include representations of the Virtual Machine. Many of the models specify that the representation includes a uri field whose value is the URI of the resource being represented. This is present to support URI discovery in nested representations.

Wenn Sie Skripte für häufige Workload-Schutz-Vorgänge schreiben möchten, verwenden Sie die in Python geschriebenen Referenzbeispiele als Orientierungshilfe. Eine Microsoft Silverlight-Anwendung wird zusammen mit dem Quellcode ebenfalls zu Referenzzwecken bereitgestellt.

API-Übersicht

PlateSpin Protect verfügt über eine REST-basierte API-Technologievorschau, die Entwickler bei der Erstellung eigener Anwendungen für das Produkt verwenden können. Die API enthält Informationen über die folgenden Vorgänge:

- Container ermitteln
- Workloads ermitteln
- Schutz konfigurieren
- Reproduktionen, Failover-Vorgänge und Failback ausführen
- Workload- und Container-Status abfragen
- Status laufender Vorgänge abfragen
- Sicherheitsgruppen und deren Schutzverbindungen

Protect-Administratoren können ein Jscript-Beispiel (`https://localhost/protectionservices/Documentation/Samples/protect.js`) von der Befehlszeile aus verwenden, um über die API auf das Produkt zuzugreifen. Anhand des Beispiels können Sie Skripte schreiben, die Ihnen die Arbeit mit dem Produkt erleichtern. Mit dem Befehlszeilenprogramm können Sie die folgenden Vorgänge durchführen:

- Einzelnen Workload hinzufügen

- Einzelnen Container hinzufügen
- Reproduktions-, Failover- und Failback-Vorgänge ausführen
- Mehrere Workloads und Container gleichzeitig hinzufügen

HINWEIS: Weitere Informationen über diesen Vorgang finden Sie in der API-Dokumentation unter `https://localhost/protectionservices/Documentation/AddWorkloadsAndContainersFromCsvFile.htm`.

- Alle Workloads gleichzeitig entfernen
- Alle Container gleichzeitig entfernen

Auf der Startseite der PlateSpin Protect REST-API (`https://localhost/protectionservices/` oder `https://<server page>/protectionservices/`) finden Sie Links zu Inhalten, die für Entwickler und Administratoren nützlich sein können.

Diese Technologievorschau wird in späteren Versionen vollständig entwickelt sein und über weitere Funktionen verfügen.

6 Hilfswerkzeuge für die Arbeit mit physischen Computern

Im Lieferumfang von PlateSpin Protect sind Werkzeuge enthalten, die für die Verwendung bei der Arbeit mit physischen Computern als Failback-Ziele vorgesehen sind.

6.1 Verwalten der Gerätetreiber

PlateSpin Protect wird mit einer Bibliothek an Gerätetreibern ausgeliefert. Die passenden Treiber werden automatisch auf den Ziel-Workloads installiert. Falls Treiber fehlen oder nicht kompatibel sind oder falls Sie für Ihre Zielinfrastruktur bestimmte Treiber benötigen, müssen Sie möglicherweise Treiber zur PlateSpin Protect-Treiberdatenbank hinzufügen (heraufladen).

In den folgenden Abschnitten finden Sie weitere Details:

6.1.1 Verpacken von Gerätetreibern für Windows-Systeme

So verpacken Sie Ihre Windows-Gerätetreiber zum Heraufladen in die PlateSpin Protect-Treiberdatenbank:

1. Bereiten Sie alle abhängigen Gerätetreiberdateien (`*.sys`, `*.inf`, `*.dll` usw.) für Ihre Zielinfrastruktur und Ihr Zielgerät vor. Wenn Sie herstellerspezifische Treiber als `.zip`-Archiv oder als Programmdatei erhalten haben, extrahieren Sie diese zuerst.
2. Speichern Sie die Treiberdateien in separaten Ordnern mit einem eigenen Ordner pro Gerät.

Die Treiber können nun hochgeladen werden. Weitere Informationen hierzu finden Sie in „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Protect“, auf Seite 100.

HINWEIS: Damit eine problemlose Durchführung Ihres Schutzauftrags und des Ziel-Workloads gewährleistet ist, sollten Sie nur digital signierte Treiber für die folgenden Systeme hochladen:

- Alle 64-Bit-Windows-Systeme
- 32-Bit-Versionen von Windows Vista- und Windows Server 2008 und Windows 7-Systemen

6.1.2 Verpacken von Gerätetreibern für Linux-Systeme

Wenn Sie ein Paket Ihrer Linux-Gerätetreiber erstellen möchten, um sie in die PlateSpin Protect-Treiberdatenbank hochzuladen, können Sie hierfür ein benutzerdefiniertes Dienstprogramm verwenden, das in Ihrem PlateSpin-ISO-Boot-Image enthalten ist.

1. Erstellen Sie auf einer Linux-Workstation ein Verzeichnis für Ihre Gerätetreiberdateien. Alle Treiber in dem Verzeichnis müssen für denselben Kernel und dieselbe Architektur sein.
2. Laden Sie das Boot-Image herunter und mounten Sie es.

   Wenn das ISO-Image beispielsweise in das Verzeichnis `/root` kopiert wurde, geben Sie den folgenden Befehl für Ziele auf BIOS- bzw. UEFI-Firmware-Basis ein:

   ```
   # mkdir /mnt/ps # mount -o loop /root/bootofx.x2p.iso /mnt/ps
   ```
3. Kopieren Sie vom Unterverzeichnis `/tools` des gemounteten ISO-Images das Archiv `packageModules.tar.gz` in ein anderes Arbeitsverzeichnis und extrahieren Sie es.

   Wenn sich beispielsweise die `.gz`-Datei in Ihrem aktuellen Arbeitsverzeichnis befindet, geben Sie folgenden Befehl ein:

   ```
   tar -xvzf packageModules.tar.gz
   ```
4. Wechseln Sie zum Arbeitsverzeichnis und führen Sie folgenden Befehl aus:

   ```
   ./PackageModules.sh -d <Pfad-zum-Treiberverzeichnis> -o <Paketname>
   ```

   Ersetzen Sie *<Pfad-zum-Treiberverzeichnis>* mit dem aktuellen Pfad zum Verzeichnis, in dem Sie Ihre Treiberdateien gespeichert haben, und *<Paketname>* mit dem aktuellen Paketnamen im folgenden Format:

   Treibername-Treiberversion-Dist-Kernelversion-Arch.pkg

   Beispiel: `bnx2x-1.48.107-RHEL4-2.6.9-11.EL-i686.pkg`

Das Paket kann nun hochgeladen werden. Weitere Informationen hierzu finden Sie unter „Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Protect“, auf Seite 100.

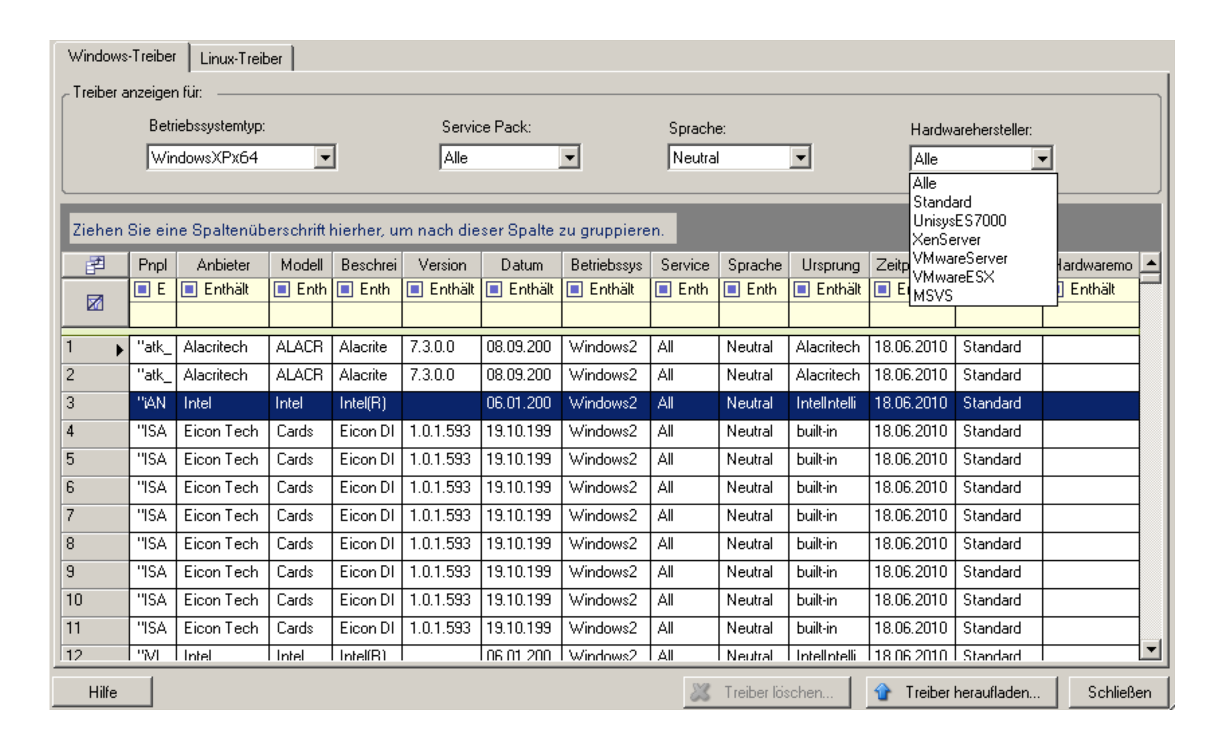
6.1.3 Hochladen von Treibern in die Gerätetreiberdatenbank von PlateSpin Protect

Verwenden Sie den PlateSpin Treibermanager zum Hochladen von Gerätetreibern in die Treiberdatenbank.

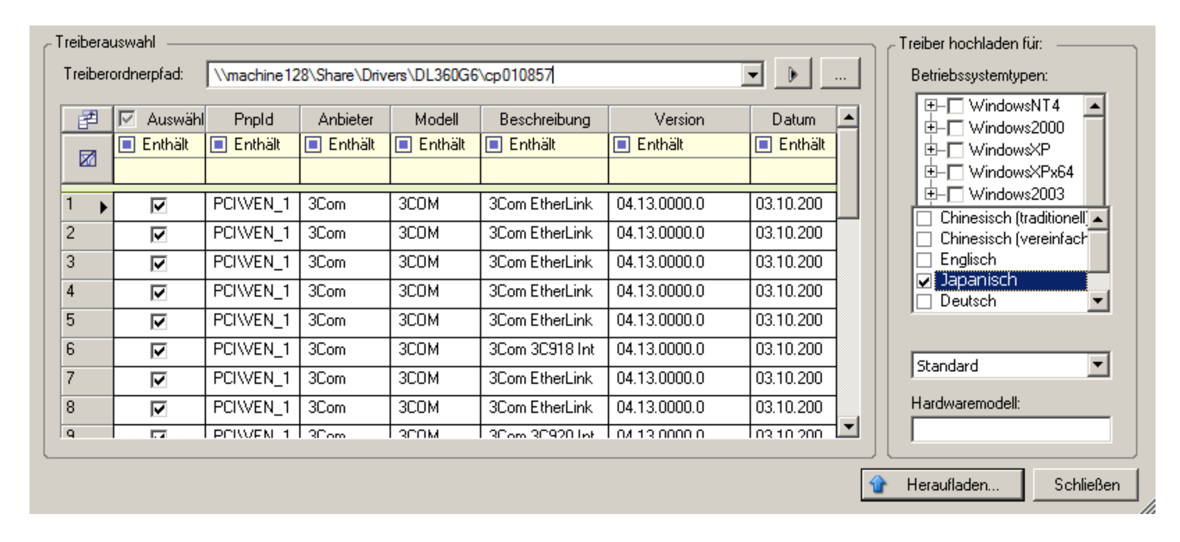
HINWEIS: Beim Heraufladen von Treibern überprüft PlateSpin Protect nicht, ob der Treiber zum ausgewählten Betriebssystem bzw. den Bit-Spezifikationen passt. Laden Sie daher nur solche Treiber herauf, die für die Zielinfrastruktur geeignet sind.

Upload-Prozedur für Gerätetreiber (Windows)

1. Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie in Verpacken von Gerätetreibern für Windows-Systeme.
2. Starten Sie auf dem PlateSpin Server-Host unter `Programme\PlateSpin Protect Server\DriverManager` das Programm `DriverManager.exe` und wählen Sie die Registerkarte **Windows-Treiber** aus.



3 Klicken Sie auf **Treiber heraufladen...**, navigieren Sie zu dem Ordner, der die erforderlichen Treiberdateien enthält, und wählen Sie den zutreffenden Betriebssystemtyp, die Sprache und die Hardwarehersteller-Optionen aus.



Wählen Sie **Standard** als Option für **Hardwarehersteller** aus, es sei denn, Ihre Treiber sind speziell für eine der aufgeführten Zielumgebungen vorgesehen.

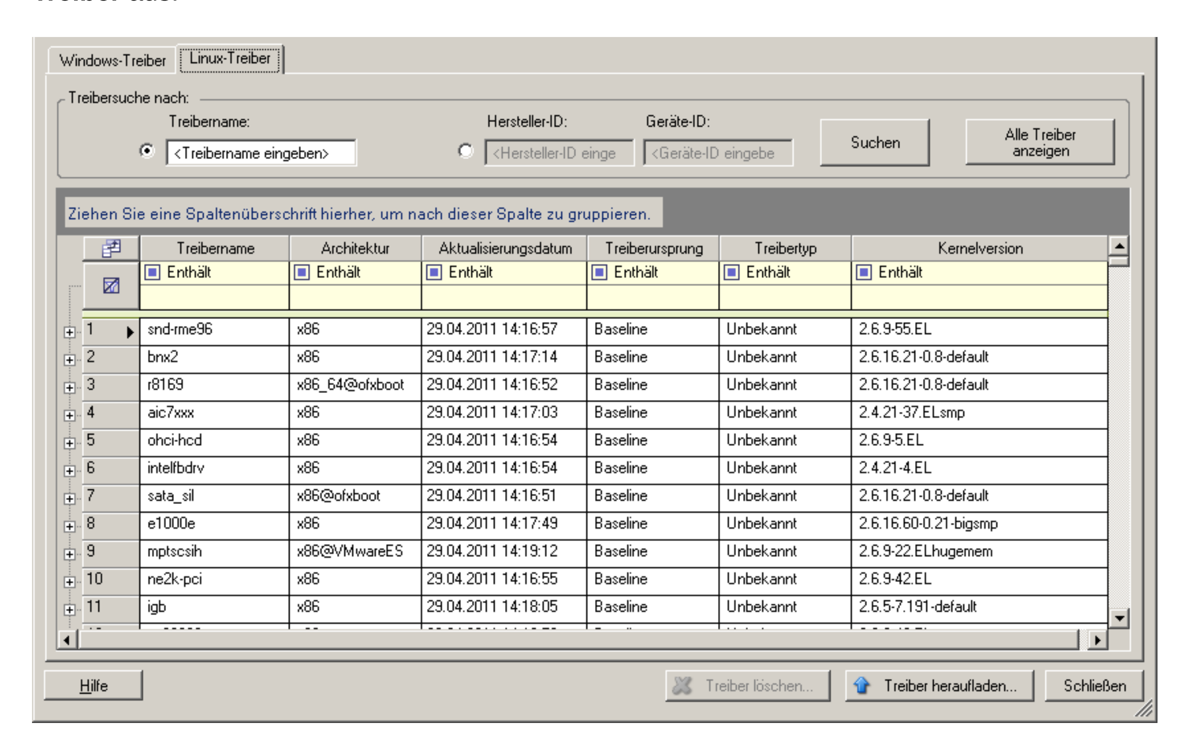
4 Klicken Sie auf **Heraufladen...** und bestätigen Sie Ihre Auswahl.

Das System lädt die ausgewählten Treiber in die Treiberdatenbank.

Upload-Prozedur für Gerätetreiber (Linux)

1 Beziehen Sie die erforderlichen Gerätetreiber und bereiten Sie diese vor. Weitere Informationen hierzu finden Sie in Verpacken von Gerätetreibern für Linux-Systeme.

2 Klicken Sie auf **Werkzeuge** > **Gerätetreiber verwalten** und wählen Sie die Registerkarte **Linux-Treiber** aus:



3 Klicken Sie auf **Treiber heraufladen...**, navigieren Sie zu dem Ordner, der das erforderliche Treiberpaket (`*.pkg`) enthält, und klicken Sie auf **Alle Treiber heraufladen**.

Das System lädt die ausgewählten Treiber in die Treiberdatenbank.

6.1.4 Verwenden der Funktion für die Plug-&-Play(PnP)-ID-Übersetzung

„Plug & Play“ (PnP) bezeichnet eine Funktion des Betriebssystems Windows, die die Konnektivität, Konfiguration und Verwaltung nativer Plug-&-Play-Geräte unterstützt. Unter Windows erleichtert diese Funktion das Auffinden von PnP-kompatiblen Hardwaregeräten, die mit einem PnP-kompatiblen Bus verbunden sind. Die Hersteller der PnP-kompatiblen Geräte weisen diesen Geräten eine Reihe von Geräteidentifikationsstrings zu. Diese Strings werden bei der Produktion in die Geräte einprogrammiert. Die Strings bilden die Grundlage der PnP-Funktionsweise: Sie sind ein Teil der Informationsquelle, mit der Windows einen geeigneten Treiber für das Gerät ermittelt.

Wenn der PlateSpin-Server die Workloads und die verfügbare Hardware ermittelt, werden diese PnP-IDs und der Speicher dieser Daten als Teil der Workload-Details festgestellt. Anhand der IDs stellt PlateSpin fest, ob und welche Treiber bei einem Failover/Failback eingefügt werden müssen. Auf dem PlateSpin-Server wird eine Datenbank der PnP-IDs mit den Treibern für alle unterstützten

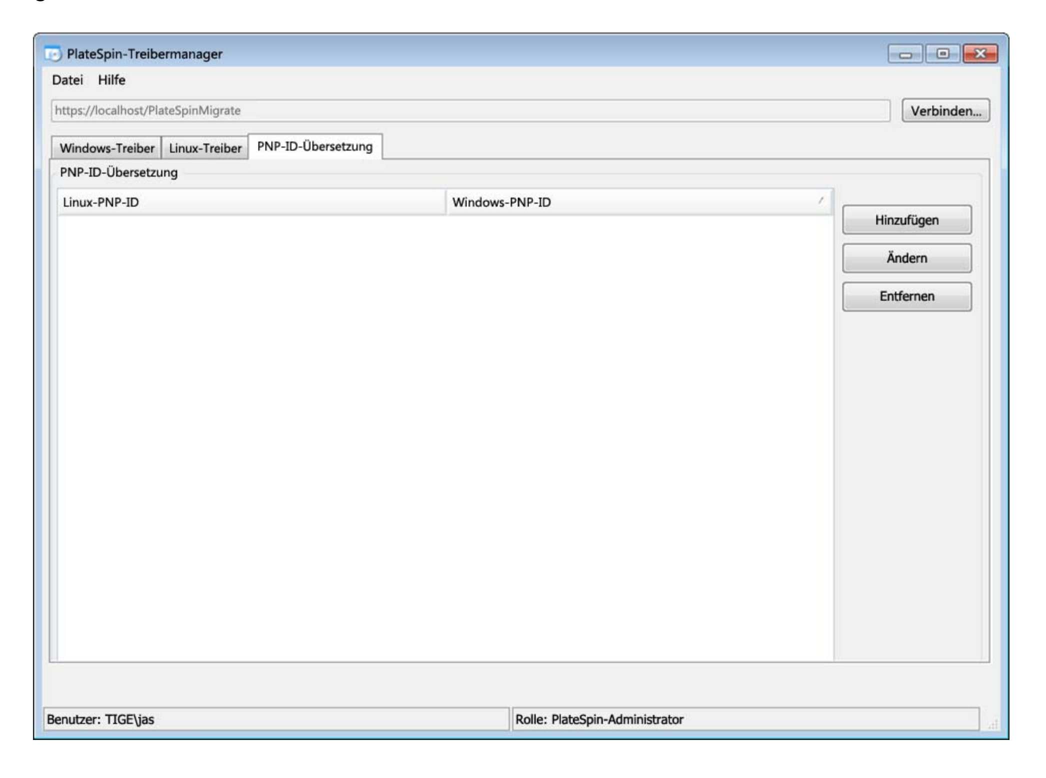
Betriebssysteme geführt. Da unter Windows und Linux unterschiedliche Formate für die PnP-IDs verwendet werden, enthält ein Windows-Workload, der vom Protect-Linux-RAM-Datenträger erkannt wird, PnP-IDs im Linux-Format.

Diese IDs sind einheitlich formatiert, so dass PlateSpin die zugehörige Windows-PnP-ID anhand der Standardumwandlung feststellen kann. Die Übersetzung erfolgt automatisch im PlateSpin-Produkt. Mit dieser Funktion sind Sie oder ein Kundendiensttechniker in der Lage, benutzerdefinierte PnP-Zuordnungen hinzuzufügen, zu bearbeiten oder zu entfernen.

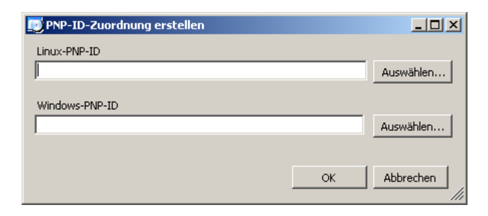
So verwenden Sie die Übersetzungsfunktion für PnP-IDs:

1 Starten Sie den PlateSpin-Treibermanager, und stellen Sie eine Verbindung zum PlateSpin-Server her.

2 Wechseln Sie im Treibermanager zur Registerkarte „PNP-ID-Übersetzung“. Die Liste **PnP-ID-Übersetzung** mit den derzeit bekannten benutzerdefinierten PnP-ID-Zuordnungen wird geöffnet.



3 Klicken Sie auf der Listenseite auf **Hinzufügen**. Das Dialogfeld „PnP-ID-Zuordnung erstellen“ wird geöffnet.



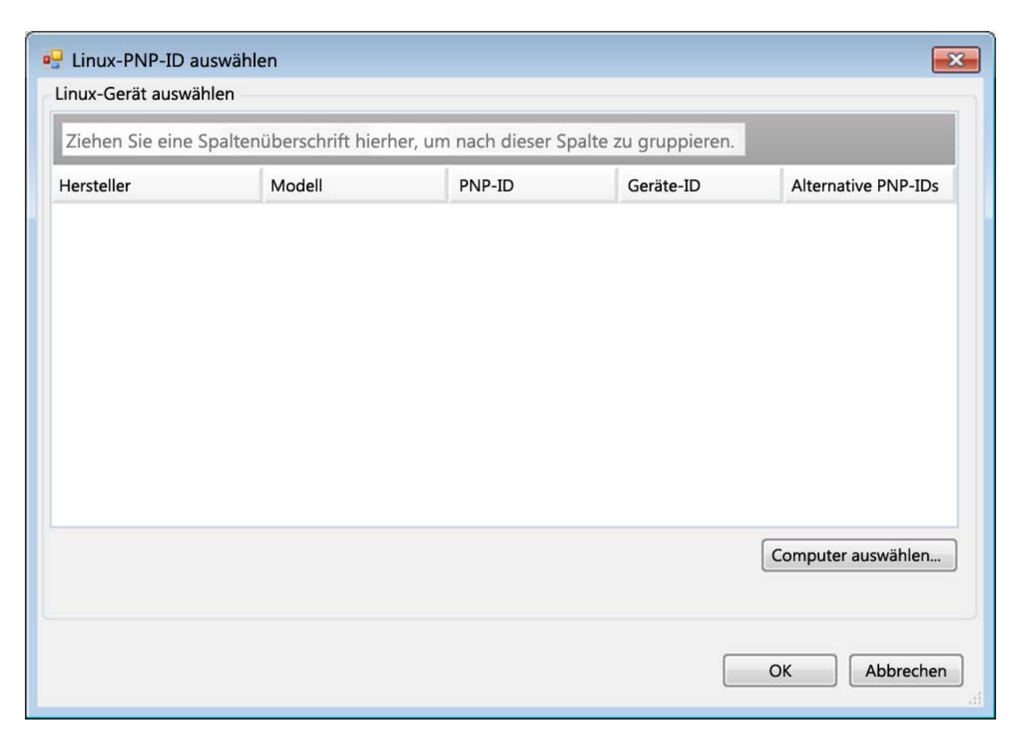
4 Fügen Sie dem Feld **Linux-PNP-ID** eine Linux-PnP-ID hinzu.

4a (Bedingt) Wenn Ihnen die Linux-PnP-ID bekannt ist, geben Sie diese ID ein.

Alternativ:

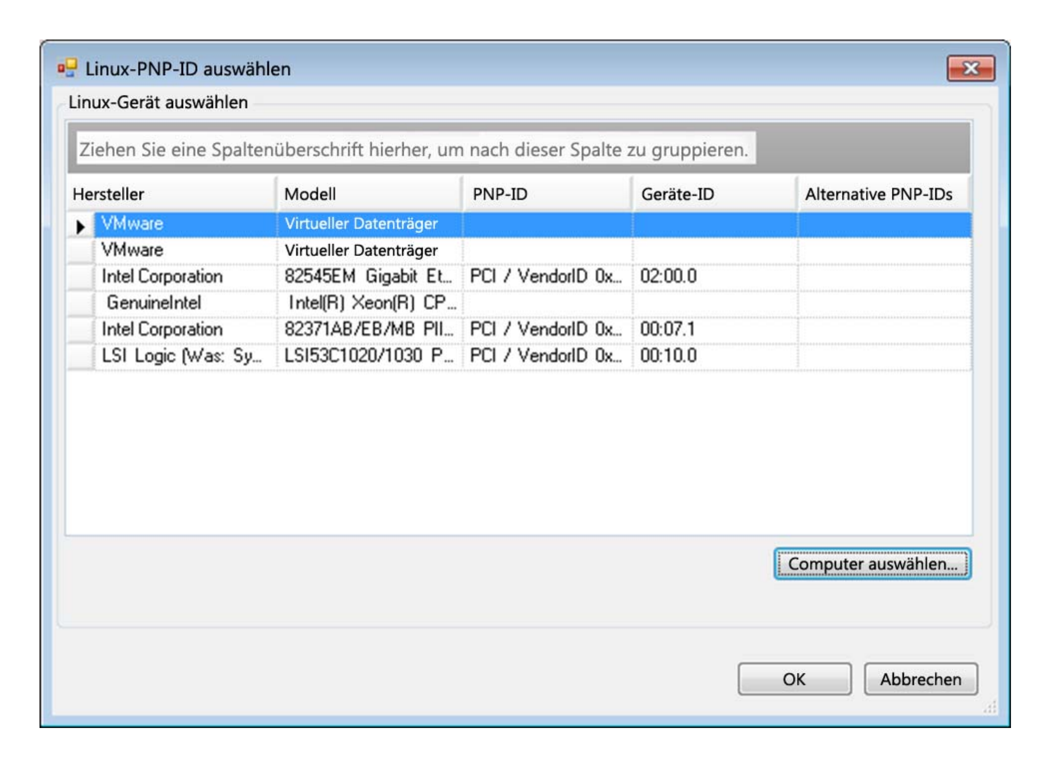
4b (Bedingt) Wählen Sie eine ID aus einem zuvor erkannten Workload aus:

4b1 Klicken Sie neben dem Feld **Linux-PNP-ID** auf **Auswählen...**. Das Dialogfeld „Linux-PNP-ID auswählen“ wird geöffnet.



4b2 Klicken Sie im Dialogfeld auf **Computer auswählen...**. Eine Liste der Computer, die zuvor durch den PlateSpin-Linux-RAM-Datenträger erkannt wurden, wird angezeigt.

4b3 Markieren Sie eines der Geräte in der Liste, und klicken Sie auf **Auswählen**. Das Gerät wird in die Liste im Dialogfeld „Linux-PNP-ID auswählen“ übernommen.



4b4 Wählen Sie ein Gerät aus der Liste aus, und klicken Sie auf **OK**. Für die PnP-ID wird die standardmäßige Umwandlung vorgenommen, und die ID wird im Dialogfeld „PnP-ID-Zuordnung erstellen“ angezeigt.

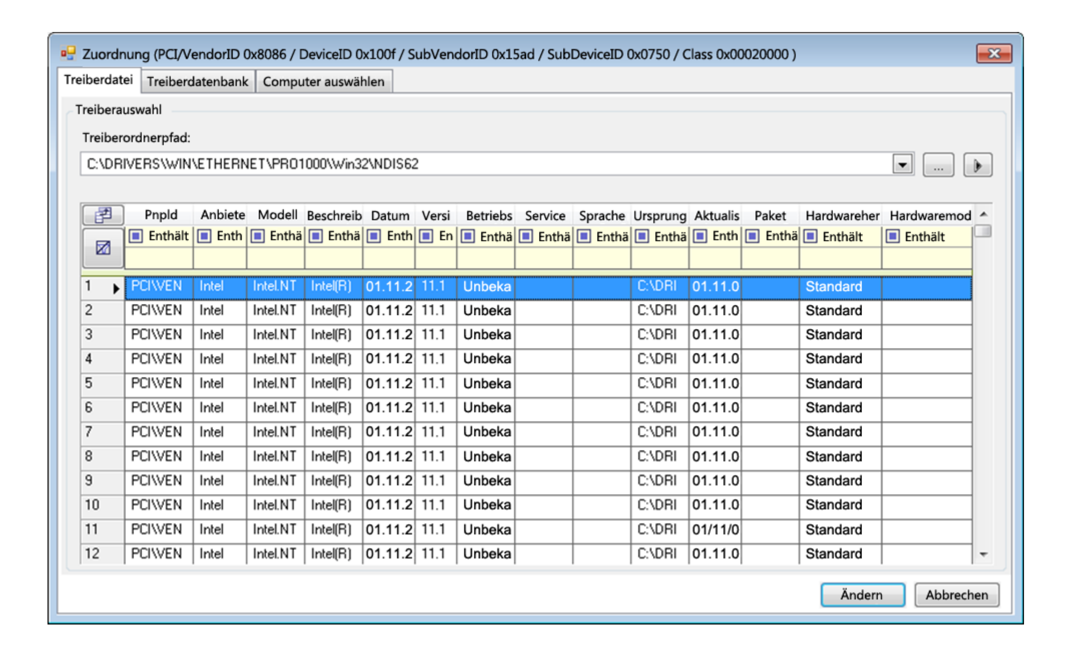
5 Fügen Sie dem Feld **Windows-PNP-ID** eine Windows-PnP-ID hinzu.

5a (Bedingt) Wenn Ihnen die Windows-PnP-ID bekannt ist, geben Sie diese ID ein.

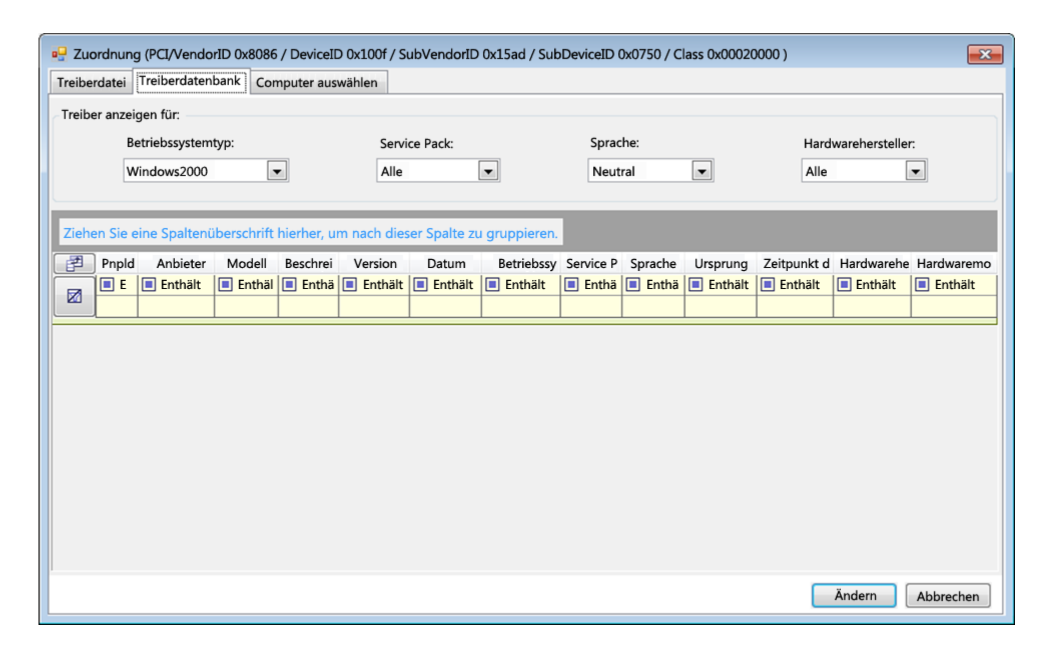
Alternativ:

5b (Bedingt) Klicken Sie neben dem Feld **Windows-PNP-ID** auf **Auswählen**. Ein Zuordnungswerkzeug wird geöffnet, in dem drei Methoden als Hilfe zum Zuordnen einer Windows-PnP-ID angeboten werden:

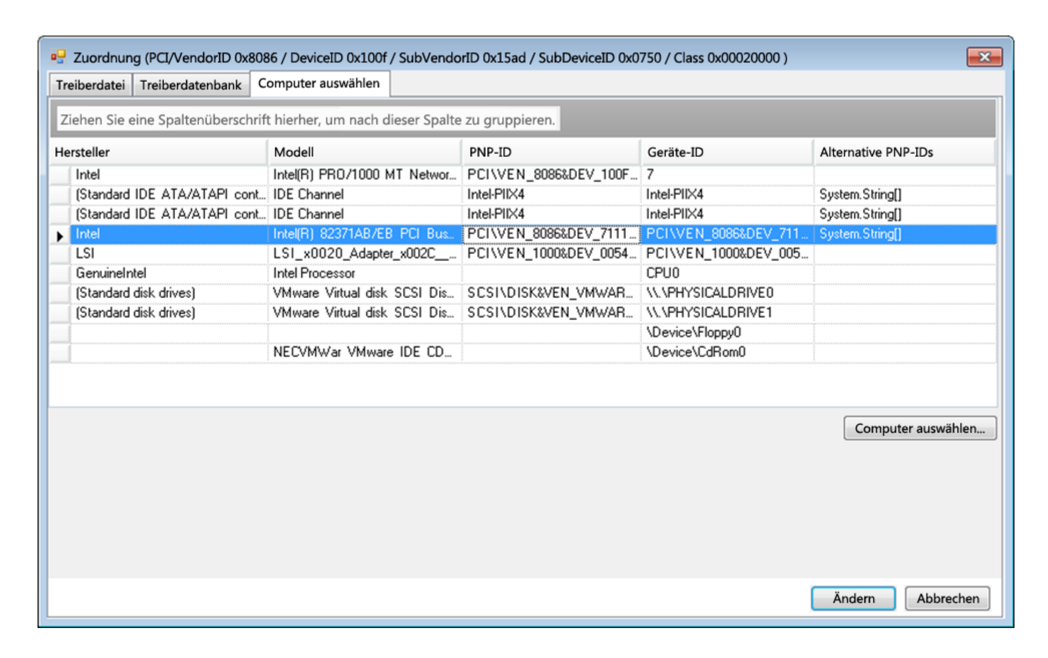
- Markieren Sie auf der Registerkarte **Treiberdatei** eine Windows-Treiberdatei (also eine Datei mit der Dateinamenerweiterung *.`inf`), wählen Sie die gewünschte PnP-ID aus, und klicken Sie auf **Ändern**.



- Markieren Sie auf der Registerkarte **Treiberdatenbank** die vorhandene Treiberdatenbank, wählen Sie die entsprechende PnP-ID aus, und klicken Sie auf **Ändern**.



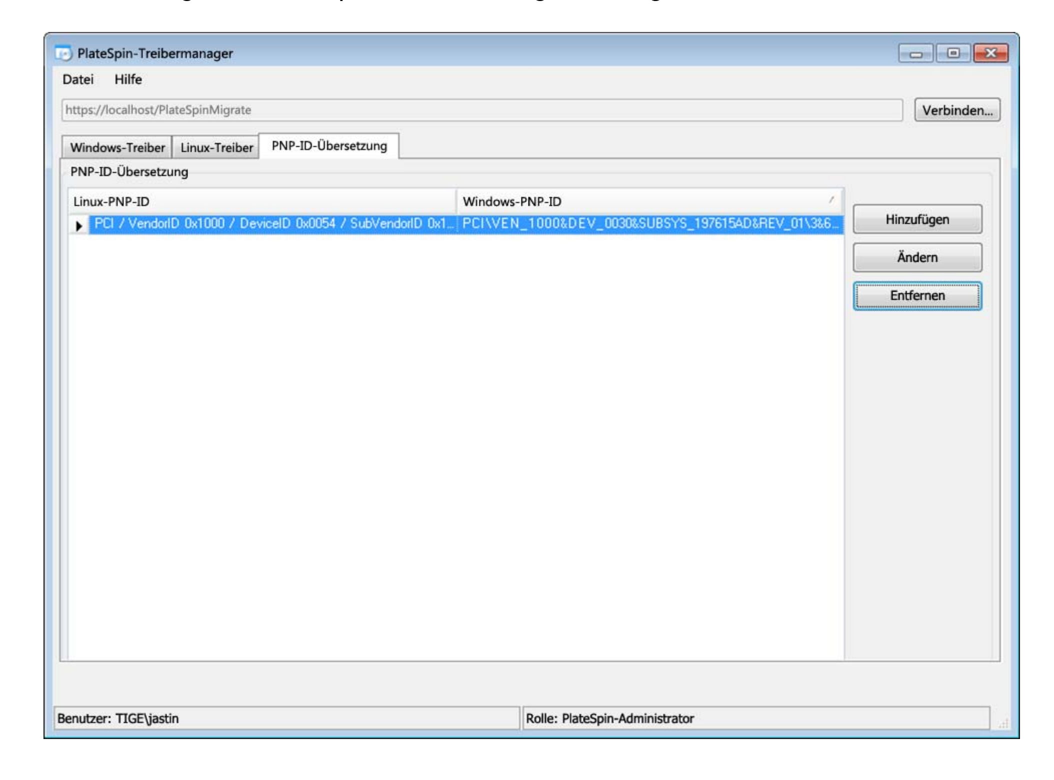
- Klicken Sie auf der Registerkarte **Computer auswählen** auf **Computer auswählen**. Wählen Sie dann in der Liste der Windows-Computer, die während der Live-Ermittlung erkannt wurden, einen Computer aus, und klicken Sie auf **OK**. Die Geräte dieses Computers werden angezeigt. Wählen Sie die gewünschte PnP-ID aus, und klicken Sie auf Ändern.



WICHTIG: Wenn Sie eine Windows-PnP-ID auswählen, die nicht mit einem Treiberpaket verknüpft ist, kann dies zum Zeitpunkt des Failover/Failback zu einem Fehler führen.

---

6 Bestätigen Sie im Dialogfeld „PnP-ID-Zuordnung erstellen“, dass die richtige Linux-PnP-ID und die richtige Windows-PnP-ID ausgewählt sind, und klicken Sie auf **OK**. Die Seite „PNP-ID-Übersetzung“ des PlateSpin-Treibermanagers wird geöffnet.



7 (Optional) Soll die Zuordnung in der Liste „PNP-ID-Übersetzung“ geändert oder entfernt werden, klicken Sie entsprechend auf **Entfernen** oder **Ändern**.

Mit **Entfernen** wird die Zuordnung gelöscht. (Zuvor wird allerdings ein Dialogfeld zur Bestätigung geöffnet.)

Zum Ändern gehen Sie wie folgt vor:

7a Klicken Sie auf **Ändern**. Das Dialogfeld „PnP-ID-Zuordnung erstellen“ wird geöffnet.

7b Wiederholen Sie Schritt 5 auf Seite 105, und bearbeiten Sie die Windows-PnP-ID.

HINWEIS: Die Linux-PnP-ID kann weder ausgewählt noch geändert werden.

---

7 ProtectAgent-Dienstprogramm

Mit dem Befehlszeilenprogramm ProtectAgent (`ProtectAgent.cli.exe`) können Sie die Treiber für die blockbasierte Übertragung installieren, aufrüsten, abfragen und deinstallieren. Beim Installieren, Deinstallieren und Aufrüsten von Treibern muss in jedem Fall ein Neustart erfolgen; mit ProtectAgent können Sie präzise steuern, wann diese Aktionen ausgeführt werden und somit wann der Server neu gestartet wird. Mit ProtectAgent ist es beispielsweise möglich, die Treiber während einer geplanten Ausfallzeit statt während der ersten Reproduktion zu installieren.

Die Syntax für das ProtectAgent-Dienstprogramm lautet:

```
ProtectAgent.cli.exe [Option] [/psserver=%IP%]
```

Tabelle 7-1 zeigt die verfügbaren Optionen und den verfügbaren Switch für den Befehl `ProtectAgent.cli.exe`.

***Tabelle 7-1** Befehlsoptionen und Switch für ProtectAgent*

Verwendung	Beschreibung
Optionen	
`h |?	help`	Zeigt die Nutzung und die Optionen für den Befehl.
`logs|view-logs`	Öffnet das Anwendungsprotokollverzeichnis.
`status`	Zeigt den Installationsstatus für den Controller und die Treiber in PlateSpin.
`din|driver-install`	Installiert die PlateSpin-Treiber.
`dup|driver-upgrade`	Rüstet die PlateSpin-Treiber auf.
`dun|driver-uninstall`	Deinstalliert die PlateSpin-Treiber.
Switch	
`/psserver=%IP%`	Lädt die Treiber für die blockbasierte Übertragung vom angegebenen Server herunter, sobald Sie die Option `status`, `driver-install` oder `driver-upgrade` aufrufen.

Eine Kopie der Treiber für die blockbasierte Übertragung ist im Bundle mit dem ProtectAgent-Dienstprogramm enthalten. Alternativ können Sie die Treiber mit dem Befehlszeilenschalter `/psserver=` vom PlateSpin-Server herunterladen, sobald Sie die Option `status`, `driver-install` oder `driver-upgrade` aufrufen. Dies ist insbesondere dann von Nutzen, wenn der Server mit einem neuen Treiberpaket gepatcht wurde, das ProtectAgent-Befehlszeilenprogramm jedoch nicht.

HINWEIS: Zur Verdeutlichung: Bei der Verwendung von ProtectAgent wird empfohlen, zunächst die Treiber zu installieren, zu deinstallieren oder aufzurüsten und dann das System vor der Reproduktion neu zu starten.

Sie sollten das System bei jedem Installieren, Aufrüsten oder Deinstallieren der Treiber neu starten. Hierdurch wird der derzeit ausgeführte Treiber angehalten, und beim Neustart des Systems wird der neue Treiber angewendet. Wenn Sie das System vor der Reproduktion nicht neu starten, verhält sich

der Ursprung weiterhin so, als wäre die Aktion nicht ausgeführt worden. Wenn Sie beispielsweise Treiber installieren und das System dann nicht neu starten, verhält sich der Ursprung so, als wären keine Treiber während der Reproduktion installiert worden. Wenn Sie die Treiber ohne Neustart aufrüsten, verwendet der Ursprung den derzeit ausgeführten Treiber entsprechend so lange weiter, bis Sie das System neu starten.

Mit der Option `Status` wird der Benutzer daran erinnert, einen Neustart vorzunehmen, falls die Version des installierten Treibers nicht mit der Version des ausgeführten Treibers identisch ist. Beispiel:

```
C:\ProtectAgent\ProtectAgent.cli.exe /status
Step 1 of 2: Querying the PlateSpin controller service
   Done
Step 2 of 2: Querying the installed PlateSpin driver version
   Done

The task completed successfully
PlateSpin Controller Service Status
    Status: Running
    Version: 9.9.9.9
    Last Successful Contact: 1/5/2015 12:14:25 PM

PlateSpin Driver Status
    Installed Driver Version: 8.0.0.11
    Running Driver Version: Not running. Reboot to load the driver.
    Upgrade Available: No
```

PlateSpin erstellt eine Aufgabe, mit der der Benutzer darauf hingewiesen wird, dass zum Abschluss der Treiberinstallation oder -aufrüstung ein Neustart erforderlich ist. Die Benachrichtigung wird in der Aufgabenliste angezeigt (Abbildung 7-1). Während der Reproduktion wird die Benachrichtigung auf der Seite „Befehlsdetails“ angezeigt (Abbildung 7-2).

***Abbildung 7-1** Aufgabe für Neustart-Benachrichtigung*

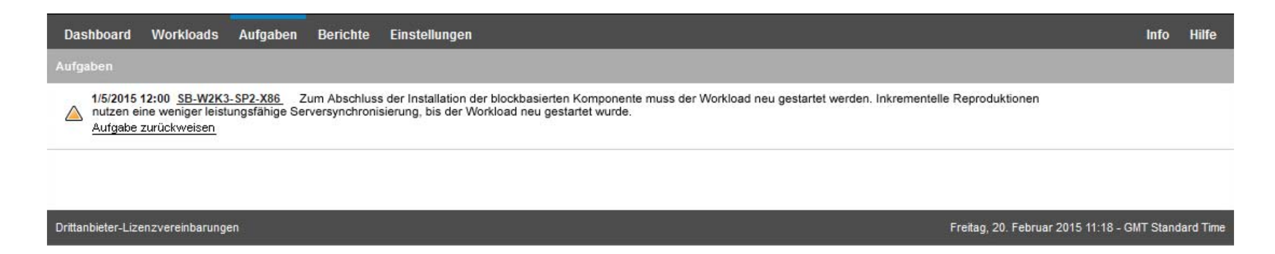
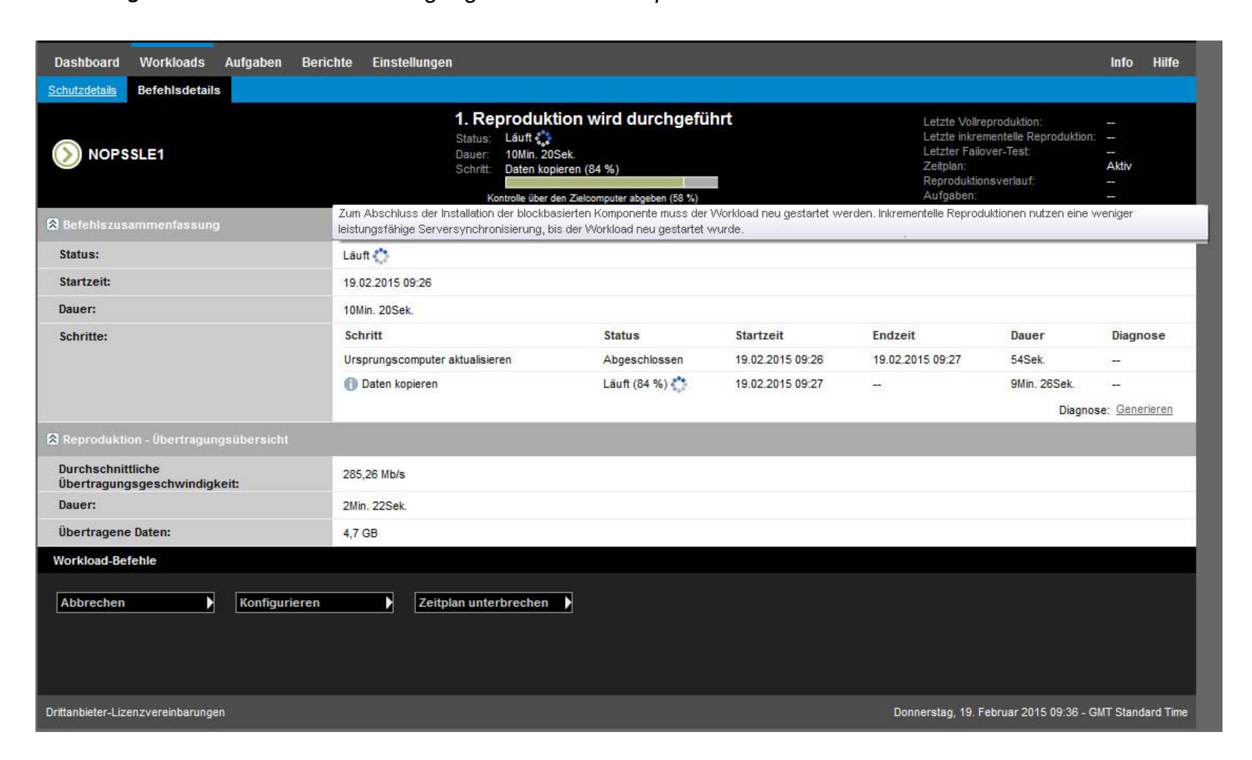
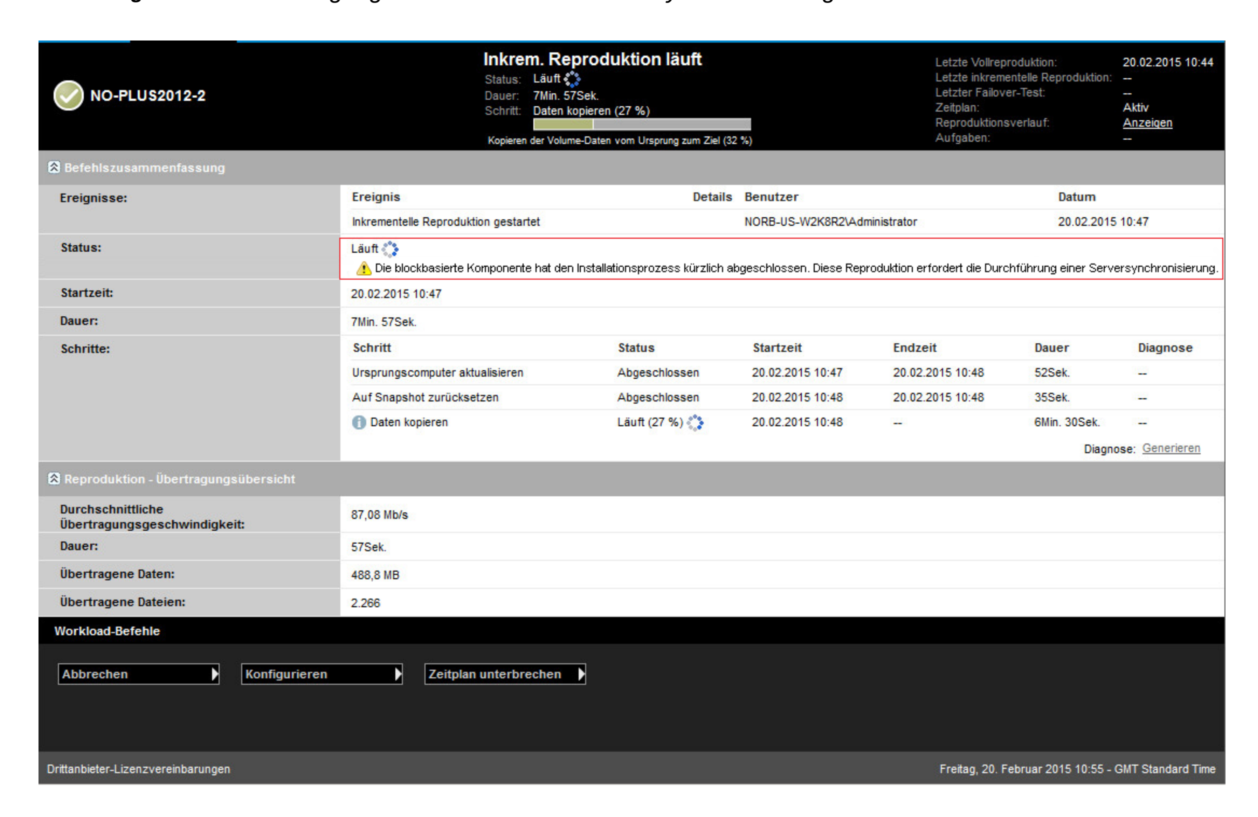


***Abbildung 7-2** Neustart-Benachrichtigung während der Reproduktion*



Beim Neustarten des Ursprungscomputers werden die installierten oder aufgerüsteten Treiber angewendet und gestartet. Wenn der Treiber erst kürzlich installiert wurde, ist nach dem Neustart eine vollständige Reproduktion bzw. eine Serversynchronisierungs-Reproduktion erforderlich, damit alle Änderungen am Ursprung erfasst werden. Diese Serversynchronisierungs-Reproduktion wird dem Benutzer im Feld „Status“ als Warnmeldung angezeigt (Abbildung 7-3). Nachfolgende inkrementelle Reproduktionen werden ohne Warnmeldung ausgeführt.

Abbildung 7-3 Benachrichtigung über erforderliche Serversynchronisierung



8 Fehlersuche

Dieser Abschnitt enthält folgende Informationen:

8.1 Fehlerbehebung bei der Workload-Inventarisierung (Windows)

Möglicherweise müssen Sie die folgenden typischen Probleme während der Workload-Inventarisierung beheben.

Probleme oder Meldungen	Lösungen
`Die Domäne in dem Berechtigungsnachweis ist ungültig oder leer.`	Dieser Fehler tritt auf, wenn das Format des Berechtigungsnachweises falsch ist. Versuchen Sie, die Ermittlung unter Verwendung eines lokalen Administratorkontos mit dem Berechtigungsnachweisformat `Hostname\LocalAdmin` durchzuführen. Sie können auch versuchen, die Ermittlung unter Verwendung eines Domänen-Administratorkontos mit dem Berechtigungsnachweisformat `Domäne\DomainAdmin` durchzuführen.
`Es konnte keine Verbindung zum Windows-Server hergestellt werden. Zugriff verweigert.`	Bei dem Versuch, einen Workload hinzuzufügen, wurde ein Nicht-Administratorkonto verwendet. Verwenden Sie ein Administratorkonto oder fügen Sie den Benutzer zur Administratorgruppe hinzu und versuchen Sie es erneut. Diese Meldung kann auch auf einen WMI-Verbindungsfehler hinweisen. Probieren Sie die nachfolgend aufgeführten Lösungsmöglichkeiten aus und führen Sie dann den „WMI-Verbindungstest“, auf Seite 115 erneut durch. Wenn der Test erfolgreich ist, versuchen Sie erneut, den Workload hinzuzufügen. • „Fehlerbehebung bei DCOM-Verbindungen“, auf Seite 115 • „Fehlerbehebung bei der RPC-Dienst-Verbindung“, auf Seite 115

Probleme oder Meldungen	Lösungen
`Es konnte keine Verbindung zum Windows-Server hergestellt werden. Netzwerkpfad nicht gefunden.`	Netzwerk-Verbindungsfehler. Führen Sie die Tests in „Durchführen von Verbindungstests“, auf Seite 114 durch. Falls ein Test fehlschlägt, stellen Sie sicher, dass sich PlateSpin Protect und der Workload im selben Netzwerk befinden. Konfigurieren Sie das Netzwerk neu und versuchen Sie es erneut.
`„Serverdetails für {hostname} ermitteln“ fehlgeschlagen. Fortschritt: 0 %. Status: NotStarted.`	Dieser Fehler kann aus verschiedenen Gründen auftreten. Es gibt für jede Ursache eine eigene Lösung: ◆ Bei Umgebungen, die einen lokalen Proxy mit Authentifizierung verwenden: Umgehen Sie den Proxy oder fügen Sie die richtigen Berechtigungen hinzu. Weitere Informationen finden Sie im Wissensdatenbankartikel 7920339. ◆ Wenn lokale Richtlinien oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im Wissensdatenbankartikel 7920862 beschriebenen Schritte aus.

Workload-Ermittlungsfehler mit Fehlermeldung
`Die Datei output.xml wurde nicht gefunden`
oder
`Netzwerkpfad nicht gefunden`
oder (beim Versuch, einen Windows-Cluster zu ermitteln)
`Inventar konnte nicht ermitteln. Als Ergebnis wurde nichts zurückgegeben.`
	Es gibt mehrere mögliche Gründe für den Fehler `Datei output.xml wurde nicht gefunden`:
	◆ Virenschutz-Software auf dem Ursprung könnte die Ermittlung beeinträchtigen. Deaktivieren Sie die Virenschutz-Software, um festzustellen, ob sie die Ursache für das Problem ist. Weitere Informationen hierzu finden Sie unter „Deaktivieren der Virenschutz-Software“, auf Seite 116.
	◆ Die Datei- und Drucker-Freigabe für Microsoft-Netzwerke ist möglicherweise nicht aktiviert. Aktivieren Sie die Freigabe in den Eigenschaften der Netzwerkschnittstellenkarte.
	◆ Die Admin$-Freigaben auf dem Ursprung sind möglicherweise nicht zugänglich. Stellen Sie sicher, dass PlateSpin Protect auf diese Freigaben zugreifen kann. Weitere Informationen hierzu finden Sie unter „Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff“, auf Seite 116.
	◆ Der Server- oder der Arbeitsstationsdienst läuft möglicherweise nicht. Wenn dies der Fall ist, aktivieren Sie den Dienst und stellen Sie den Startmodus auf `Automatisch` ein.
	◆ Der Remoteregistrierungsdienst von Windows ist deaktiviert. Starten Sie den Dienst und stellen Sie den Starttyp auf „Automatisch“ ein.

In den folgenden Abschnitten finden Sie weitere Informationen zur Fehlersuche bei Windows-Workloads:

- Abschnitt 8.1.1, „Durchführen von Verbindungstests“, auf Seite 114
- Abschnitt 8.1.2, „Deaktivieren der Virenschutz-Software“, auf Seite 116
- Abschnitt 8.1.3, „Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff“, auf Seite 116

8.1.1 Durchführen von Verbindungstests

- „Netzwerk-Verbindungstest“, auf Seite 115
- „WMI-Verbindungstest“, auf Seite 115
- „Fehlerbehebung bei DCOM-Verbindungen“, auf Seite 115
- „Fehlerbehebung bei der RPC-Dienst-Verbindung“, auf Seite 115

Netzwerk-Verbindungstest

Führen Sie diesen allgemeinen Netzwerk-Verbindungstest durch, um festzustellen, ob PlateSpin Protect mit dem Workload kommunizieren kann, den Sie zu schützen versuchen.

1. Wechseln Sie zu Ihrem PlateSpin Server-Host.
2. Öffnen Sie ein Befehlszeilenfenster und senden Sie einen Ping-Befehl an Ihren Workload:

   `ping` *Workload-IP-Adresse*

WMI-Verbindungstest

1. Wechseln Sie zu Ihrem PlateSpin Server-Host.
2. Klicken Sie auf **Start > Ausführen**, geben Sie `Wbemtest` ein und drücken Sie die `Eingabetaste`.
3. Klicken Sie auf **Verbinden**.
4. Geben Sie unter **Namespace** den Namen des Workloads ein, den Sie zu ermitteln versuchen, und hängen Sie `\root\cimv2` an den Namen an. Wenn der Hostname beispielsweise `win2k` lautet, geben Sie Folgendes ein:

   `\\win2k\root\cimv2`
5. Geben Sie den entsprechenden Berechtigungsnachweis ein. Verwenden Sie hierzu entweder das Format `Hostname\LocalAdmin` oder `Domäne\DomainAdmin`.
6. Klicken Sie auf **Verbinden**, um die WMI-Verbindung zu testen.

   Wenn eine Fehlermeldung zurückgegeben wird, kann keine WMI-Verbindung zwischen PlateSpin Protect und Ihrem Workload hergestellt werden.

Fehlerbehebung bei DCOM-Verbindungen

1. Melden Sie sich bei dem zu schützenden Workload an.
2. Klicken Sie auf **Start > Ausführen**.
3. Geben Sie `dcomcnfg` ein und drücken Sie die Eingabetaste.
4. Prüfen Sie die Verbindung:
   - Bei Windows-Systemen (XP/Vista/2003/2008/7) wird das Fenster „Komponentendienste“ angezeigt. Klicken Sie im Ordner **Computer** des Konsolenbaums im Verwaltungstool „Komponentendienste“ mit der rechten Maustaste auf den Computer, den Sie hinsichtlich der DCOM-Verbindung prüfen möchten, und klicken Sie anschließend auf **Eigenschaften**. Klicken Sie auf die Registerkarte **Standardeigenschaften** und stellen Sie sicher, dass **DCOM (Distributed COM) auf diesem Computer aktivieren** ausgewählt ist.
   - Auf einem Computer am Windows 2000-Server wird das Dialogfeld „DCOM-Konfiguration“ angezeigt. Klicken Sie auf die Registerkarte **Standardeigenschaften** und stellen Sie sicher, dass **DCOM (Distributed COM) auf diesem Computer aktivieren** ausgewählt ist.
5. Wenn DCOM nicht aktiviert ist, aktivieren Sie es und booten Sie entweder den Server neu oder starten Sie den Windows-Verwaltungsinstrumentation-Dienst neu. Versuchen Sie nun nochmals, den Workload hinzuzufügen.

Fehlerbehebung bei der RPC-Dienst-Verbindung

Es gibt drei potenzielle Blockaden beim RPC-Dienst:

- Der Windows-Dienst

- Eine Windows-Firewall
- Eine Netzwerk-Firewall

Stellen Sie für den Windows-Dienst sicher, dass der RPC-Dienst auf dem Workload ausgeführt wird. Führen Sie `services.msc` von einem Befehlszeilenfenster aus, um das Dienstefenster zu öffnen. Fügen Sie für eine Windows-Firewall eine RPC-Ausnahme hinzu. Bei Hardware-Firewalls können Sie folgende Strategien probieren:

- PlateSpin Protect und der Workload müssen sich auf derselben Seite der Firewall befinden
- Öffnen spezifischer Ports zwischen PlateSpin Protect und dem Workload (siehe „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 29)

8.1.2 Deaktivieren der Virenschutz-Software

Virenschutz-Software kann gelegentlich einige der PlateSpin Protect-Funktionen blockieren, die sich auf WMI und die Remote-Registrierung beziehen. Um sicherzustellen, dass das Workload-Inventar erfolgreich ist, kann es nötig sein, den Virenschutz-Service an einem Workload zunächst zu deaktivieren. Darüber hinaus kann Virenschutz-Software mitunter auch den Zugriff auf bestimmte Dateien sperren und nur den Zugriff auf bestimmte Prozesse oder Programmdateien zulassen. Dies kann mitunter die dateibasierte Datenreproduktion verhindern. Wenn Sie den Workload-Schutz konfigurieren, können Sie in diesem Fall die zu deaktivierenden Dienste auswählen, z. B. Dienste, die von Virenschutz-Software installiert und verwendet werden. Diese Dienste werden nur für die Dauer der Dateiübertragung deaktiviert. Sobald der Prozess abgeschlossen ist, werden sie wieder gestartet. Bei einer Datenreproduktion auf Blockebene ist dies nicht erforderlich.

8.1.3 Aktivieren von Datei-/Freigabe-Berechtigungen und -Zugriff

Für den zuverlässigen Schutz eines Workloads muss PlateSpin Protect erfolgreich Software innerhalb des Workloads bereitstellen und installieren. Bei der Bereitstellung dieser Komponenten auf einem Workload sowie während des Hinzufügens eines Workloads verwendet PlateSpin Protect die administrativen Freigaben des Workloads. PlateSpin Protect benötigt Administratorzugriff auf die Freigaben und verwendet dazu ein lokales Administratorkonto oder ein Domänen-Administratorkonto.

So stellen Sie sicher, dass die administrativen Freigaben aktiviert sind:

1. Klicken Sie mit der rechten Maustaste auf **Arbeitsplatz** auf dem Desktop und wählen Sie **Verwalten**.
2. Erweitern Sie **System > Freigegebene Ordner > Freigaben**.
3. Im Verzeichnis `Freigegebene Ordner` müsste neben anderen die Freigabe Admin$ vorhanden sein.

Nachdem Sie sich vergewissert haben, dass die Freigaben aktiviert sind, stellen Sie sicher, dass sie vom PlateSpin Server-Host aus zugänglich sind:

1. Wechseln Sie zu Ihrem PlateSpin Server-Host.
2. Klicken Sie auf **Start > Ausführen**, geben Sie `\\<Server-Host>\Admin$` ein und klicken Sie anschließend auf **OK**.
3. Verwenden Sie bei Aufforderung denselben Berechtigungsnachweis wie für das Hinzufügen des Workloads zum PlateSpin Protect-Workload-Inventar.

   Das Verzeichnis wird geöffnet und Sie sollten in der Lage sein, darin zu navigieren und seinen Inhalt zu ändern.

4 Wiederholen Sie diesen Vorgang für alle Freigaben außer der IPC$-Freigabe.

Windows verwendet die IPC$-Freigabe für die Berechtigungsnachweisvalidierung und Authentifizierung. Sie ist nicht einem Ordner oder einer Datei im Workload zugeordnet, der Test schlägt daher immer fehl. Die Freigabe sollte aber weiterhin sichtbar sein.

PlateSpin Protect ändert den vorhandenen Inhalt des Volumes nicht. Es erstellt jedoch ein eigenes Verzeichnis, für das es Zugriff und Berechtigungen benötigt.

8.2 Fehlerbehebung bei der Workload-Inventarisierung (Linux)

Probleme oder Meldungen	Lösungen
`Es konnte weder eine Verbindung zum SSH-Server, der auf <IP-Adresse> läuft, noch zu den VMware Virtual Infrastructure-Webdiensten unter <IP-Adresse>/sdk hergestellt werden.`	Diese Meldung wird aufgrund mehrerer möglicher Ursachen ausgegeben: ◆ Der Workload ist nicht erreichbar. ◆ Auf dem Workload wird SSH nicht ausgeführt. ◆ Die Firewall ist aktiv und die erforderlichen Ports wurden nicht geöffnet. ◆ Das spezifische Betriebssystem des Workloads wird nicht unterstützt Informationen zu Netzwerk- und Zugriffsanforderungen für einen Workload finden Sie unter „Zugriffs- und Kommunikationsanforderungen in Ihrem Schutz-Netzwerk“, auf Seite 29.
`Zugriff verweigert.`	Dieses Authentifizierungsproblem weist auf einen ungültigen Benutzernamen oder ein ungültiges Passwort hin. Weitere Informationen über den richtigen Berechtigungsnachweis für den Workload-Zugriff finden Sie unter „Richtlinien für Workload- und Container-Berechtigungsnachweise“, auf Seite 76.

8.3 Beheben von Problemen während der Ausführung des Befehls „Reproduktion vorbereiten“ (Windows)

Probleme oder Meldungen	Lösungen
Authentifizierungsfehler beim Überprüfen der Controller-Verbindung während der Einrichtung des Controllers auf dem Ursprung.	Das für das Hinzufügen eines Workloads verwendete Konto muss von dieser Richtlinie zugelassen sein. Weitere Informationen hierzu finden Sie unter „Gruppenrichtlinie und Benutzerrechte“, auf Seite 118.

Probleme oder Meldungen	Lösungen
Es konnte nicht festgestellt werden, ob .NET Framework installiert ist (mit Ausnahme `Die vertrauenswürdige Beziehung zwischen dieser Arbeitsstation und der primären Domäne ist fehlgeschlagen`).	Überprüfen Sie, ob der Remoteregistrierungsdienst auf dem Ursprung aktiviert ist und ausgeführt wird. Siehe auch „Fehlerbehebung bei der Workload-Inventarisierung (Windows)“, auf Seite 113.

8.3.1 Gruppenrichtlinie und Benutzerrechte

Aufgrund der Art und Weise, wie PlateSpin Protect mit dem Betriebssystem des Ursprungs-Workloads interagiert, muss das zum Hinzufügen des Workloads verwendete Administratorkonto über bestimmte Benutzerrechte auf dem Ursprungscomputer verfügen. In den meisten Fällen sind diese Einstellungen Standardwerte der Gruppenrichtlinie. Wenn die Umgebung jedoch gesperrt wurde, wurden folgende Benutzerrechte-Zuweisungen möglicherweise entfernt:

- Traverse Checking umgehen
- Token auf Prozessebene ersetzen
- Als Teil des Betriebssystems agieren

Um zu überprüfen, ob diese Gruppenrichtlinien-Einstellungen festgelegt wurden, können Sie `gpresult /v` von der Befehlszeile auf dem Ursprungscomputer oder alternativ `RSOP.msc` ausführen. Wenn die Richtlinie nicht festgelegt oder wenn sie deaktiviert wurde, kann sie über die lokale Sicherheitsrichtlinie des Computers oder über eine der für den Computer geltenden Domänengruppenrichtlinien aktiviert werden.

Sie können die Richtlinie sofort mithilfe von `gpupdate /force` (bei Windows 2003/XP) oder `secedit /refreshpolicy machine_policy /enforce` (bei Windows 2000) aktualisieren.

8.4 Fehlerbehebung bei der Workload-Reproduktion

Probleme oder Meldungen	Lösungen
Behebbarer Fehler bei der Reproduktion während des Vorgangs **Erstellen eines Snapshots der virtuellen Maschine planen** oder **Planen des Zurücksetzens der virtuellen Maschine auf Snapshot vor dem Start**.	Dieses Problem tritt auf, wenn der Server ausgelastet ist und der Vorgang länger als erwartet dauert. Warten Sie bis die Reproduktion abgeschlossen ist.

Probleme oder Meldungen	Lösungen
Workload-Problem erfordert Benutzereingriff.	Diese Meldung kann von verschiedenen Problemen verursacht worden sein. In den meisten Fällen sollte die Meldung weitere Angaben zur Art des Problems und dem Problembereich (wie Konnektivität, Berechtigungsnachweis etc.) enthalten. Warten Sie nach der Fehlersuche einige Minuten. Wenden Sie sich an den PlateSpin-Support, falls die Meldung weiterhin angezeigt wird.
Bei allen Workloads treten behebbare Fehler auf, da kein Speicherplatz mehr vorhanden ist.	Überprüfen Sie den freien Speicherplatz. Wenn mehr Platz erforderlich ist, entfernen Sie einen Workload.
Langsame Netzwerkgeschwindigkeiten unter 1 MB.	Stellen Sie sicher, dass die Duplex-Einstellung der Netzwerkschnittstellenkarte des Ursprungscomputers aktiviert ist und dass der Switch, mit dem sie verbunden ist, eine entsprechende Einstellung hat. Wenn der Switch auf automatisch gesetzt ist, kann der Ursprung nicht auf 100 MB eingestellt werden.
Langsame Netzwerkgeschwindigkeiten über 1 MB.	Messen Sie die Latenz, indem Sie folgenden Befehl vom Ursprungs-Workload aus ausführen: `ping` *`ip`* `-t` (ersetzen Sie *ip* durch die IP-Adresse Ihres PlateSpin Server-Hosts). Lassen Sie den Befehl für 50 Iterationen ausführen. Der Durchschnitt gibt dann die Latenz an. Siehe auch „Optimieren des Datentransfers über WAN-Verbindungen“, auf Seite 40.

`Die Dateiübertragung kann nicht beginnen - Port 3725 wird bereits verwendet`
 	
oder
 	
`3725 - Herstellen einer Verbindung nicht möglich`
	Stellen Sie sicher, dass der Port offen ist und überwacht:
	
	Führen Sie `netstat -ano` auf dem Workload aus.
	
	Überprüfen Sie die Firewall.
	
	Wiederholen Sie die Reproduktion.

`Controller-Verbindung nicht hergestellt` Die Reproduktion schlägt beim Schritt **Kontrolle über die virtuelle Maschine übernehmen** fehl.	Dieser Fehler tritt auf, wenn die Reproduktionsnetzwerkinformationen ungültig sind. Entweder ist der DHCP-Server nicht verfügbar oder das virtuelle Reproduktionsnetzwerk kann keine Verbindung zum PlateSpin Server-Host herstellen. Ändern Sie die Reproduktions-IP in eine statische IP oder aktivieren Sie den DHCP-Server. Stellen Sie sicher, dass das für die Reproduktion ausgewählte virtuelle Netzwerk eine Verbindung zum PlateSpin Server-Host herstellen kann.

Probleme oder Meldungen	Lösungen
Der Reproduktionsauftrag startet nicht (hängt bei 0 %)	Dieser Fehler kann aus unterschiedlichen Gründen auftreten. Es gibt für jede Ursache eine eigene Lösung: ◆ Bei Umgebungen, die einen lokalen Proxy mit Authentifizierung verwenden: Umgehen Sie den Proxy oder fügen Sie die richtigen Berechtigungen hinzu, um dieses Problem zu beheben. Weitere Informationen finden Sie im Wissensdatenbankartikel 7920339. ◆ Wenn lokale Richtlinien oder Domänenrichtlinien die erforderlichen Berechtigungen einschränken, führen Sie die im Wissensdatenbankartikel 7920862 beschriebenen Schritte aus. Dieses Problem tritt häufig auf, wenn der PlateSpin Server-Host mit einer Domäne verbunden ist und die Domänenrichtlinien mit Einschränkungen angewendet werden. Weitere Informationen hierzu finden Sie unter „Gruppenrichtlinie und Benutzerrechte“, auf Seite 118.
Nach einer Windows-Aktualisierung werden einige Dateien im Ordner `C:\Windows\SoftwareDistribution` während der schrittweisen dateibasierten Reproduktion nicht an den Zielcomputer übertragen.	Dies ist eine allgemeine Vorgehensweise von Microsoft Windows: Zum Zweck der Optimierung werden einige Dateien für die Löschung im Registrierungsschlüssel `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot` markiert, um zu verhindern, dass sie in VSS-Snapshots integriert werden. Weitere Informationen finden Sie im Microsoft Developer Network-Artikel *Ausschließen von Dateien von Schattenkopien*. Im Allgemeinen werden diese Dateien vor der Löschung zur Installation von Windows-Aktualisierungen verwendet und sind nach der Aktualisierung nicht mehr erforderlich. Falls Sie diese Dateien wiederherstellen möchten, führen Sie die Windows-Aktualisierung nach dem Failover auf dem Zielcomputer aus, um den Ordner `SoftwareDistribution` neu zu füllen.

8.5 Fehlersuche bei Workloads, die Datenverkehr weiterleiten

In einigen Szenarien führt die Reproduktion eines Workloads, der Netzwerkverkehr weiterleitet (wenn der Zweck des Workloads beispielsweise darin liegt, als Netzwerk-Bridge für NAT, VPN oder eine Firewall zu dienen), zu einer deutlichen Verminderung der Netzwerkleistung. Dies hängt mit einem Problem mit VMXNET 2- und VMXNET 3-Adaptern zusammen, bei denen LRO (Large Receive Offload) aktiviert ist.

Zur Umgehung dieses Problems müssen Sie LRO am virtuellen Netzwerkadapter deaktivieren. Weitere Informationen finden Sie im Wissensdatenbankartikel 7005495.

8.6 Fehlersuche bei der Online-Hilfe

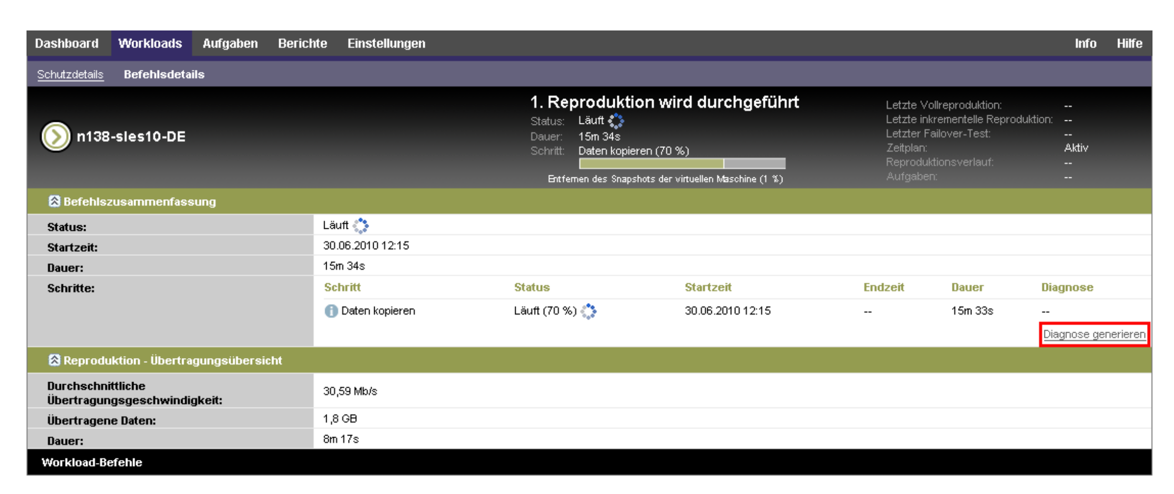
Auf einigen Systemen mit erweiterten Browser-Sicherheitseinstellungen (z. B. Internet Explorer 8 auf Windows Server 2008) funktionieren die Symbole zum Erweitern und Komprimieren (+ und -) im Inhaltsverzeichnis möglicherweise nicht. Aktivieren Sie zur Behebung des Problems in Ihrem Browser JavaScript:

- **Internet Explorer:** Klicken Sie auf **Extras > Internetoptionen > Registerkarte „Sicherheit“** > **Zone „Internet“** > **Stufe anpassen** und wählen Sie anschließend die Option **Aktivieren** für die **Active Scripting**-Funktion aus.
- **Firefox:** Klicken Sie auf die Registerkarte **Extras > Optionen > Inhalt** und wählen Sie anschließend die Option **JavaScript aktivieren** aus.

8.7 Generieren und Anzeigen von Diagnoseberichten

Nachdem Sie auf der PlateSpin Protect-Weboberfläche einen Befehl ausgeführt haben, können Sie detaillierte Diagnoseberichte über die Details des Befehls generieren.

1 Klicken Sie auf **Befehlsdetails** und dann auf **Diagnose generieren**.



Nach kurzer Zeit wird die Seite aktualisiert und zeigt den Link **Ansicht** oberhalb des Links **Diagnose generieren** an.

2 Klicken Sie auf **Anzeigen**.

Es wird eine neue Seite mit umfassenden Diagnoseinformationen zum aktuellen Befehl geöffnet.

3 Speichern Sie die Diagnoseseite und halten Sie sie bereit, falls Sie den technischen Support kontaktieren müssen.

8.8 Entfernen von Workloads

In einigen Situationen müssen Sie einen Workload unter Umständen vom PlateSpin Protect-Inventar entfernen und später wieder hinzufügen.

1 Wählen Sie auf der Seite „Workloads“ den zu entfernenden Workload aus und klicken Sie anschließend auf **Workload entfernen**.

(Bedingt) Bei Windows-Workloads, die zuvor durch eine Reproduktion auf Blockebene geschützt wurden, werden Sie auf der PlateSpin Protect Weboberfläche aufgefordert, anzugeben, ob Sie auch die blockbasierten Komponenten entfernen möchten. Folgenden Optionen stehen zur Auswahl:

- **Komponenten nicht entfernen:** Die Komponenten werden nicht entfernt.
- **Komponenten entfernen, Workload aber nicht neu starten:** Die Komponenten werden entfernt. Es ist jedoch ein Neustart des Workloads erforderlich, um den Deinstallationsprozess abzuschließen.
- **Komponenten entfernen und Workload neu starten:** Die Komponenten werden entfernt und der Workload wird automatisch neu gestartet. Dieser Vorgang muss während der geplanten Ausfallzeit durchgeführt werden.

2 Klicken Sie auf der Seite „Befehlsbestätigung“ auf **Bestätigen**, um den Befehl auszuführen.

Warten Sie, bis der Vorgang abgeschlossen ist.

8.9 Workload-Bereinigung nach dem Schutz

Befolgen Sie diese Schritte, um Ihren Ursprungs-Workload von allen PlateSpin-Software-Komponenten zu bereinigen, falls dies erforderlich ist, wie z. B. nach einem erfolglosen oder problematischen Schutz.

Die entsprechenden Informationen finden Sie in den folgenden Abschnitten:

- Abschnitt 8.9.1, „Bereinigen von Windows-Workloads“, auf Seite 122
- Abschnitt 8.9.2, „Bereinigen von Linux-Workloads“, auf Seite 123

8.9.1 Bereinigen von Windows-Workloads

Komponente	Entfernungsanweisung
Blockbasierte PlateSpin-Übertragungskomponente	Weitere Informationen hierzu finden Sie im Knowledgebase-Artikel 7005616.
Blockbasierte Übertragungskomponente eines Drittanbieters (eingestellt)	1. Windows Software-Applet verwenden (`appwiz.cpl` ausführen) und die Komponenten entfernen. Abhängig vom Ursprung haben Sie eine der folgenden Versionen: ◆ SteelEye Data Replication for Windows v6 Update2 ◆ SteelEye DataKeeper For Windows v7 2. Booten Sie den Computer neu.
Dateibasierte Übertragungskomponente	Auf Root-Ebene für jedes geschützte Volume alle Dateien namens `PlateSpinCatalog*.dat` entfernen.
Workload-Inventarisierungssoftware	Im `Windows`-Verzeichnis des Workloads: ◆ Alle Dateien namens `machinediscovery*` entfernen. ◆ Unterverzeichnis `platespin` entfernen.

Komponente	Entfernungsanweisung
Controller-Software	1. Eine Eingabeaufforderung öffnen und das aktuelle Verzeichnis ändern in: ◆ `\Programme\platespin*` (32-Bit-Systeme) ◆ `\Programme (x86)\platespin`* (64-Bit-Systeme) 2. Führen Sie den folgenden Befehl aus: `ofxcontroller.exe /uninstall` 3. Verzeichnis `platespin*` entfernen.

8.9.2 Bereinigen von Linux-Workloads

Komponente	Entfernungsanweisung
Controller-Software	◆ Diese Prozesse stoppen: ◆ `pkill -9 ofxcontrollerd` ◆ `pkill -9 ofxjobexec` ◆ Das OFX-Controller-rpm-Package entfernen: `rpm -e ofxcontrollerd` ◆ Im Dateisystem des Workloads das Verzeichnis `/usr/lib/ofx` mit Inhalt entfernen.

Software für den Datentransfer auf Blockebene	1. Prüfen Sie, ob der Treiber aktiv ist:
	`lsmod | grep blkwatch`
	Wenn der Treiber immer noch im Arbeitsspeicher geladen ist, sollte das Ergebnis eine Zeile wie die folgende enthalten:
	`blkwatch_7616 70924 0`
	2. (Bedingt) Wenn der Treiber noch geladen ist, entfernen Sie ihn aus dem Arbeitsspeicher:
	`rmmod blkwatch_7616`
	3. Entfernen Sie den Treiber aus der Boot-Sequenz:
	`blkconfig -u`
	4. Entfernen Sie die Treiberdateien, indem Sie das folgende Verzeichnis mitsamt Inhalt löschen:
	`/lib/modules/`*[Kernel-Version]*`/Platespin`
	5. Löschen Sie die folgende Datei:
	`/etc/blkwatch.conf`

Komponente	Entfernungsanweisung
LVM-Snapshots	LVP-Snapshots, die bei fortlaufenden Reproduktionen verwendet werden, werden entsprechend einer `Volume-Name-PS-snapshot`-Konvention benannt. Beispiel: Ein Snapshot eines `LogVol01`-Volumes wird `LogVol01-PS-snapshot` genannt. So entfernen Sie diese LVM-Snapshots: 1. Erstellen Sie anhand einer der folgenden Methoden eine Liste der Snapshots auf dem erforderlichen Workload: ◆ Erstellen Sie auf der PlateSpin Protect-Weboberfläche einen Job-Bericht für den fehlgeschlagenen Job. Der Bericht sollte Informationen über die LVM-Snapshots und deren Namen enthalten. - ODER - ◆ Führen Sie am erforderlichen Linux-Workload den folgenden Befehl aus, um eine Liste aller Volumes und Snapshots anzuzeigen: `# lvdisplay -a` 2. Notieren Sie sich die Namen und Standorte der Snapshots, die entfernt werden sollen. 3. Entfernen Sie die Snapshots mit dem folgenden Befehl: `lvremove` *Snapshot-Name*
Bitmap-Dateien	Bei jedem geschützten Volume im Volume-Stamm die entsprechende `.blocks_bitmap`-Datei entfernen.
Werkzeuge	Im Ursprungs-Workload unter `/sbin` folgende Dateien entfernen: ◆ `bmaputil` ◆ `blkconfig`

8.10 Verkleinern der PlateSpin Protect-Datenbanken

Sobald die PlateSpin Protect-Datenbanken (OFX, PortabilitySuite und Protection) eine vordefinierte Kapazität erreichen, werden diese Datenbanken in regelmäßigen Abständen bereinigt. Falls Sie die Größe oder den Inhalt dieser Datenbanken noch weitergehend steuern möchten, können Sie sie mit einem speziellen Protect-Dienstprogramm (`PlateSpin.DBCleanup.exe`) weiter bereinigen und verkleinern. Im Wissensdatenbankartikel 7006458 finden Sie Angaben zum Speicherort und den verfügbaren Optionen für dieses Werkzeug, mit denen Sie Offline-Datenbankvorgänge ausführen können.

A Von Protect unterstützte Linux-Distributionen

Die PlateSpin Protect-Software umfasst vorkompilierte Versionen des `blkwatch`-Treibers für viele fehlerfreie Linux-Verteilungen (32-Bit und 64-Bit). Dieser Abschnitt enthält folgende Informationen:

- Abschnitt A.1, „Analysieren Ihres Linux-Workloads“, auf Seite 125
- Abschnitt A.2, „Vorkompilierter „blkwatch“-Treiber (Linux)“, auf Seite 126

A.1 Analysieren Ihres Linux-Workloads

Bevor Sie feststellen können, ob PlateSpin Forge einen `blkwatch`-Treiber für Ihre Distribution umfasst, benötigen Sie weitere Informationen über den Kernel Ihres Linux-Workloads, sodass Sie ihn in der Liste der unterstützten Distributionen als Suchbegriff verwenden können. Dieser Abschnitt enthält folgende Informationen:

- Abschnitt A.1.1, „Ermitteln der Versionszeichenkette“, auf Seite 125
- Abschnitt A.1.2, „Ermitteln der Architektur“, auf Seite 125

A.1.1 Ermitteln der Versionszeichenkette

Sie können die Versionszeichenkette des Kernels Ihres Linux-Workloads ermitteln, indem Sie auf dem Linux-Terminal des Workloads den folgenden Befehl ausführen:

```
uname -r
```

Wenn Sie beispielsweise den Befehl `uname -r` ausführen, wird die folgende Zeichenkette ausgegeben:

```
3.0.76-0.11-default
```

Wenn Sie die Liste der Verteilungen durchsuchen, werden für diese Zeichenkette zwei Übereinstimmungen angezeigt:

- `SLES11SP3-GA-3.0.76-0.11-default-x86`
- `SLES11SP3-GA-3.0.76-0.11-default-x86_64`

Die Suchergebnisse geben an, dass für das Produkt Treiber sowohl für die 32-Bit-(x86)- als auch für die 64-Bit-(x86_64)-Architektur vorhanden sind.

A.1.2 Ermitteln der Architektur

Sie können die Architektur Ihrer Linux-Workloads ermitteln, indem Sie auf dem Linux-Terminal des Workloads den folgenden Befehl ausführen:

```
uname -m
```

Wenn Sie beispielsweise den Befehl `uname -m` ausführen, wird die folgende Zeichenkette ausgegeben:

```
x86-64
```

Mit dieser Information können Sie festlegen, dass der Workload über eine 64-Bit-Architektur verfügt.

A.2 Vorkompilierter „blkwatch“-Treiber (Linux)

Die folgende Liste enthält fehlerfreie Linux-Distributionen, für die Protect einen `blkwatch`-Treiber umfasst. Sie können die Liste durchsuchen, um zu ermitteln, ob die Version und Architektur des Kernels Ihres Linux-Workloads mit einer unterstützten Verteilung in der Liste übereinstimmt. Wird Ihre Version und Architektur gefunden, bietet PlateSpin Protect eine vorkonfigurierte Version des `blkwatch`-Treibers.

Ist die Suche erfolglos, können Sie einen benutzerdefinierten `blkwatch`-Treiber erstellen. Führen Sie dazu die im Wissensdatenbankartikel 7005873 beschriebenen Schritte aus.

Liste mit Elementsyntax

Jedes Element in der Liste wird mit der folgenden Syntax formatiert:

```
<Distro>-<Patch>-<Kernel_Versionszeichenkette>-<Kernel_Architektur>
```

Für eine SLES 9 SP1-Verteilung mit einer Kernelversionszeichenkette `2.6.5-7.139-bigsmp` für die 32-Bit-(x86)-Architektur wird das Element in folgendem Format aufgeführt:

```
SLES9-SP1-2.6.5-7.139-bigsmp-x86
```

Liste der Verteilungen

Eine Liste der unterstützten Kernel-Distributionen finden Sie unter „Liste der Verteilungen“ im *PlateSpin Protect-Benutzerhandbuch*.

B Synchronisieren von Seriennummern im lokalen Clusterknoten-Speicher

In diesem Abschnitt finden Sie detaillierte Informationen zu dem Vorgang, mit dem Sie lokale Volume-Seriennummern ändern können, damit sie mit den einzelnen Knoten des zu schützenden Windows-Clusters übereinstimmen. Die Informationen umfassen die Verwendung des Volume Manager-Programms `VolumeManager.exe`) für die Synchronisierung von Seriennummern im lokalen Clusterknoten-Speicher.

So laden Sie das Dienstprogramm herunter und führen es aus:

1. Suchen Sie auf der NetIQ Downloads-Website nach dem Produkt PlateSpin Protect, und klicken Sie auf **Anfrage absenden**.
2. Wählen Sie auf der Registerkarte „Produkte" die Option PlateSpin Protect 11.1. Die produktspezifische Download-Seite wird geöffnet. Klicken Sie dann auf **Mit dem Download fortfahren**.
3. Klicken Sie auf der Download-Seite in der Zeile **VolumeManager.exe** auf `Herunterladen` oder wählen Sie den entsprechenden Download-Manager-Link aus.
4. Laden Sie das Dienstprogramm herunter und kopieren Sie es anschließend für jeden Clusterknoten an einen Speicherort, auf den zugegriffen werden kann.
5. Öffnen Sie im aktiven Knoten des Clusters eine administrative Eingabeaufforderung, navigieren Sie zu dem Speicherort des heruntergeladenen Dienstprogramms und führen Sie folgenden Befehl aus:

   ```
   VolumeManager.exe -l
   ```

   Eine Liste mit den lokalen Volumes und deren entsprechenden Seriennummern wird angezeigt. Beispiel:

   ```
   Volume Listing:

   --------------------

   DriveLetter (*:) VolumeId="System Reserved" SerialNumber: AABB-CCDD

   DriveLetter (C:) VolumeId=C:\ SerialNumber: 1122-3344
   ```

   Notieren Sie sich diese Seriennummern oder lassen Sie sie angezeigt, um sie später zu vergleichen.
6. Überprüfen Sie, ob alle Seriennummern im lokalen Speicher des aktiven Knotens mit den Seriennummern im lokalen Speicher der jeweils anderen Knoten im Cluster übereinstimmen.

   6a Führen Sie in jedem Clusterknoten den Befehl `VolumeManager.exe -l` aus, um dessen Volume-Seriennummern abzurufen.

   6b Vergleichen Sie die Seriennummern im lokalen Speicher des aktiven Knotens (Schritt 5) mit den Seriennummern im lokalen Speicher des Knotens (Schritt 6a).

6c (Bedingt) Wenn sich die Seriennummern des aktiven Knotens von denen dieses Knotens unterscheiden, notieren Sie sich die Seriennummer, die Sie in diesem Knoten eintragen möchten und führen Sie den folgenden Befehl aus, um die Seriennummer festzulegen und anschließend zu überprüfen:

```
VolumeManager -s <VolumeId> <Seriennummer>
```

Nachfolgend sehen Sie zwei Beispiele, wie dieser Befehl verwendet werden könnte:

- `VolumeManager -s "Reserviertes System" AAAA-AAAA`
- `VolumeManager -s C:\ 1111-1111`

6d Wenn Sie alle Volume-Seriennummern im Knoten eines Clusters geändert haben, müssen Sie diesen Knoten neu starten.

6e Wiederholen Sie Schritt 6a bis Schritt 6d für jeden Knoten im Cluster.

7 (Bedingt) Wenn der Cluster bereits in einer PlateSpin-Umgebung geschützt wurde, empfehlen wir Ihnen, eine vollständige Reproduktion im aktiven Knoten durchzuführen, um sicherzustellen, dass alle Änderungen in der Datenbank eingetragen werden.

C Anpassen der PlateSpin Protect-Weboberfläche an das Markenbild

Sie können das Erscheinungsbild der PlateSpin Protect-Webkonsole an das Markenbild Ihres Unternehmens anpassen (z. B. Farben, Logo und Produktname). Hierbei können Sie sogar die Links zu den Registerkarten **Info** und **Hilfe** aus der Produktbenutzeroberfläche entfernen.

In diesem Abschnitt finden Sie weitere Informationen zur Bearbeitung des Markenbilds für das Produkt:

C.1 Anpassen der Benutzeroberfläche an das Markenbild mithilfe von Konfigurationsparametern

Wie andere Aspekte des Verhaltens des PlateSpin-Servers können Sie auch das Erscheinungsbild der Weboberfläche anhand von Konfigurationsparametern steuern, die Sie auf einer Konfigurationswebseite mit Ihrem PlateSpin-Server-Host (`https://`*`Ihr_PlateSpin-Server`*`/platespinconfiguration/`) festlegen. Mit diesen Parametern verleihen Sie der PlateSpin Protect-Weboberfläche das unverkennbare „Erscheinungsbild“ Ihres eigenen Unternehmens. In diesem Abschnitt finden Sie Informationen zum Ausführen dieser Anpassungen an das Marktbild.

Gehen Sie wie folgt vor, um Konfigurationsparameter zu ändern oder anzuwenden:

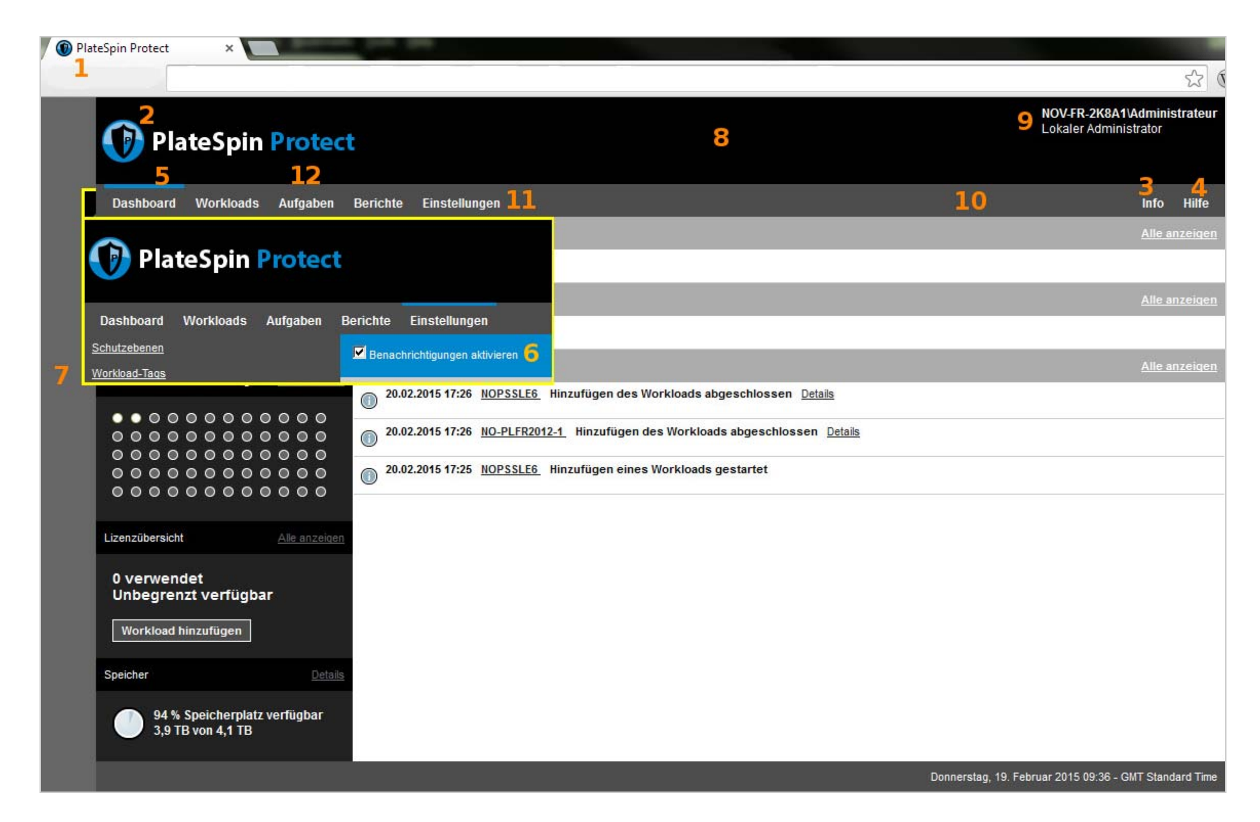
1. Öffnen Sie `https://`*`Ihr_PlateSpin-Server`*`/platespinconfiguration/` in einem beliebigen Webbrowser, und melden Sie sich als Administrator an.
2. Suchen Sie den gewünschten Serverparameter, klicken Sie auf **Bearbeiten**, und ändern Sie den Wert dieses Parameters.

   Weitere Informationen finden Sie in Abbildung C-1 sowie unter dem Namen, der Beschreibung und dem Standardwert für die Einstellungen der verschiedenen bearbeitbaren Elemente.
3. Speichern Sie die Einstellungen und schließen Sie die Seite.

   Ein Neustart des Systems oder der Services ist nach einer Änderung im Konfigurationsprogramm nicht erforderlich; es kann allerdings bis zu 30 Sekunden dauern, bis die Änderung in der Benutzeroberfläche in Kraft tritt.

Die verschiedenen Seiten der Weboberfläche weisen einige gemeinsame Erscheinungsbildelemente auf. In der Darstellung des PlateSpin Protect-Dashboards in Abbildung C-1 sind die bearbeitbaren Elemente mit Zahlen gekennzeichnet.

***Abbildung C-1** PlateSpin Protect-Weboberfläche mit Kennzeichnung der konfigurierbaren Elemente (kleinere Zusatzabbildung eingefügt)*



Die nachfolgende Tabelle zeigt die Nummer („ID“) des gekennzeichneten Elements der Benutzeroberfläche im obigen Bildschirmfoto sowie den Namen, die Beschreibung und den Standardwert der jeweils zugehörigen Einstellung. Legen Sie diese Werte auf dem PlateSpin-Server auf der Seite der Konfigurationseinstellungen gemäß dem gewünschten neuen Erscheinungsbild fest. (Klicken Sie hierzu auf der Einstellungsseite bei dem gewünschten Konfigurationswert auf **Bearbeiten**.)

ID	Konfigurationsparameter und Beschreibung	Standardwert

1	`WebUIFaviconUrl`
	
	Speicherort einer gültigen `.ico`-Grafikdatei. Wählen Sie eine der folgenden Optionen aus:
	
	◆ Gültige URL zur entsprechenden `.ico`-Datei auf einem anderen Computer.
	
	Beispiel: https://meinserver.beispiel.de/dir1/dir2/icons/meinefirma_favsymbol.ico
	
	◆ Relativer Pfad unterhalb des Stammverzeichnisses des lokalen Webservers, in das Sie die entsprechende `.ico`-Datei hochgeladen haben.
	
	Sie haben beispielsweise den Pfad `\meinefirma\images\icons` im Stammverzeichnis des Webservers erstellt, in dem die Grafikdateien für die benutzerdefinierten Symbole gespeichert werden sollen:
	
	`~/\meinefirma\images\icons\meinefirma_favsymbol.ico`
	
	Der tatsächliche Dateisystempfad, in dem sich die Datei befindet, lautet in diesem Beispiel `C:\Programme (x86)\PlateSpin Protect Server\PlateSpin Forge\web\meinefirma\images\icons\meinefirma_favsymbol.ico`.
		`~/doc/de/favicon.ico` [1]

2	`WebUILogoUrl` Speicherort der Grafikdatei mit dem Produktlogo. Wählen Sie eine der folgenden Optionen aus: ◆ Gültige URL zur entsprechenden Grafikdatei auf einem anderen Computer. Beispiel: https://meinserver.beispiel.de/dir1/dir2/logos/meinefirma_logo.png ◆ Relativer Pfad unterhalb des Stammverzeichnisses des lokalen Webservers, in das Sie die entsprechende Grafikdatei heraufgeladen haben. Sie haben beispielsweise den Pfad `meinefirma\images\logos` im Stammverzeichnis des Webservers erstellt, in dem die benutzerdefinierten Logobilder gespeichert werden sollen: `~/meinefirma/images/logos/meinefirma_logo.png`. Der tatsächliche Dateisystempfad, in dem sich die Datei befindet, lautet in diesem Beispiel `C:\Programme (x86)\PlateSpin Protect Server\PlateSpin Forge\web\meinefirma\images\logos\meinefirma_logo.png`.	`~/Resources/protectLogo.png` [2]

ID	Konfigurationsparameter und Beschreibung	Standardwert
3	`WebUIShowAboutTab` Aktiviert oder deaktiviert die Anzeige der Registerkarte **Info** (**wahr** bzw. **falsch**).	Wahr
4	`WebUIShowHelpTab` Aktiviert oder deaktiviert die Anzeige der Registerkarte **Hilfe** (**wahr** bzw. **falsch**).	Wahr
5	`WebUISiteAccentColor` Akzentfarbe (hexadezimaler RGB-Wert).	#0088CE
6	`WebUISiteAccentFontColor` Schriftfarbe für die Anzeige mit der Akzentfarbe in der Weboberfläche (hexadezimaler RGB-Wert).	#FFFFFF
7	`WebUISiteBackgroundColor` Farbe für den Hintergrund der Website (hexadezimaler RGB-Wert).	#666666
8	`WebUISiteHeaderBackgroundColor` Farbe für den Hintergrund des Website-Headers (hexadezimaler RGB-Wert).	#000000
9	`WebUISiteHeaderFontColor` Schriftfarbe für den Website-Header in der Weboberfläche (hexadezimaler RGB-Wert)	#FFFFFF
10	`WebUISiteNavigationBackgroundColor` Farbe für den Hintergrund der Website-Navigation in der Weboberfläche (hexadezimaler RGB-Wert).	#4D4D4D
11	`WebUISiteNavigationFontColor` Schriftfarbe für die Links der Website-Navigation in der Weboberfläche (hexadezimaler RGB-Wert).	#FFFFFF
12	`WebUISiteNavigationLinkHoverBackgroundColor` Farbe für den Hintergrund der Links der Websitenavigation in der Weboberfläche (hexadezimaler RGB-Wert).	#808080

[1] Der tatsächliche Dateipfad lautet `C:\Programme (x86)\PlateSpin Protect Server\PlateSpin Forge\web\doc\de\favicon.ico`.

[2] Der tatsächliche Dateipfad lautet `C:\Programme (x86)\PlateSpin Protect Server\PlateSpin Forge\web\Resources\protectLogo.png`.

C.2 Anpassen des Produktnamens an das Markenbild in der Windows-Registrierungsdatenbank

Der Titel oben in der Produktoberfläche bietet genügend Platz für ein Unternehmenslogo und für den Namen des Produkts selbst. Mithilfe eines Konfigurationsparameters können Sie das Logo ändern, das in der Regel den Produktnamen enthält. Soll der Produktname auf einer Browser-Registerkarte geändert oder entfernt werden, müssen Sie die Windows-Registrierungsdatenbank bearbeiten.

So ändern Sie den Produktnamen:

1 Führen Sie auf dem PlateSpin-Server den Befehl `regedit` aus.

2 Navigieren Sie im Windows-Registrierungs-Editor zu folgendem Registrierungsschlüssel:

   `HKEY_LOCAL_MACHINE\SOFTWARE\PlateSpin\ProtectServer\Produktname`.

   HINWEIS: Unter Umständen finden Sie diesen Registrierungsschlüssel hier:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PlateSpin\Protect`.

   ---

3 Doppelklicken Sie auf den Schlüssel `ProductName`, ändern Sie die **Datenwerte** nach Wunsch, und klicken Sie auf **OK**.

4 Starten Sie den IIS-Server neu, damit die Änderung an der Benutzeroberfläche in Kraft tritt.

Glossar

Angestrebte Testzeit (TTO). Ein Maß dafür, wie einfach sich ein Wiederherstellungsplan für den Katastrophenfall testen lässt. Es entspricht weitgehend der RTO, umfasst jedoch auch die Zeit, die ein Benutzer zum Testen des Failover-Workloads benötigt.

Angestrebte Wiederherstellungszeit (RTO). Ein Wert für die tolerierbare Ausfallzeit eines Workloads, definiert durch die Zeit, die für einen Failover-Vorgang erforderlich ist.

Angestrebter Wiederherstellungszeitpunkt (RPO). In Zeit gemessener tolerierbarer Datenverlust, der durch ein konfigurierbares Intervall zwischen inkrementellen Reproduktionen eines geschützten Workloads definiert wird.

Container. Die Workload-Schutzinfrastruktur von PlateSpin Protect, wie beispielsweise ein VM-Host.

Ereignis. Eine PlateSpin Server-Nachricht, die Informationen über wichtige Schritte während des gesamten Workload-Schutz-Lebenszyklus enthält.

Erneut schützen. Ein PlateSpin Protect-Befehl, der einen Schutzvertrag für einen Workload nach Failover- und Failback-Vorgängen wiederherstellt.

Failback. Die Wiederherstellung der Geschäftsfunktion eines fehlgeschlagenen Workloads in seiner ursprünglichen Umgebung, wenn die Geschäftsfunktion eines temporären Failover-Workloads in PlateSpin Protect nicht mehr benötigt wird.

Failover. Die Übernahme der Geschäftsfunktion eines fehlgeschlagenen Workloads von einem Failover-Workload innerhalb eines PlateSpin Protect-VM-Containers.

Failover testen. Ein PlateSpin Protect-Vorgang, bei dem ein Failover-Workload in einer isolierten Netzwerkumgebung gebootet wird, um die Funktionalität des Failovers zu testen und um die Integrität des Wiederherstellungs-Workloads zu überprüfen.

Failover-Workload. Die bootfähige virtuelle Reproduktion eines geschützten Workloads.

inkrementell. 1. (Substantiv) Eine einzelne geplante oder manuelle Übertragung von Unterschieden zwischen einem geschützten Workload und dessen Reproduktion (dem Failover-Workload).

2. (Adjektiv) Beschreibt den Umfang der *Reproduktion (1)*, in dem die anfängliche Reproduktion eines Workloads differentiell erstellt wird (auf der Basis von Unterschieden zwischen dem Workload und seinem vorbereiteten Gegenstück.

Reproduktion. 1. *Ursprüngliche Reproduktion*, die Erstellung einer ursprünglichen Basiskopie eines Workloads. Kann als *Vollständige Reproduktion* ausgeführt werden (alle Workload-Daten werden an einen „leeren" virtuellen Failover-Computer übertragen) oder als eine *Inkrementelle Reproduktion* (weitere Informationen hierzu finden Sie unter dem Punkt inkrementell (2)).

2. Jegliche Übertragung geänderter Daten von einem geschützten Workload auf seine Reproduktion im Container.

Reproduktionszeitplan. Der zur Steuerung der Häufigkeit und des Umfangs von Reproduktionen eingerichtete Zeitplan.

Schutzebene. Eine benutzerdefinierbare Sammlung an Workload-Schutz-Parametern, die die Häufigkeit von Reproduktionen definiert sowie die Kriterien festlegt, anhand derer das System einen Workload als fehlgeschlagen erachtet.

Schutzvertrag. Eine Sammlung aktuell aktiver Einstellungen, die sich auf den gesamten Lebenszyklus eines Workload-Schutzes beziehen (*Inventar hinzufügen*, ursprüngliche und fortlaufende *Reproduktionen*, *Failover*, *Failback* und *Erneut schützen*).

Ursprung. Ein Workload oder dessen Infrastruktur, der bzw. die der Ausgangspunkt für einen PlateSpin Protect-Vorgang ist. Beispielsweise ist der Ursprung beim anfänglichen Schutz eines Workloads der Produktions-Workload. Bei einem Failback-Vorgang ist es der Failover-Workload im Container.

Siehe auch Ziel.

Vorbereiten auf Failover. Ein PlateSpin Protect-Vorgang, der den Failover-Workload in Vorbereitung eines vollständigen Failover-Vorgangs bootet.

Wiederherstellungspunkt. Ein zu einem bestimmten Zeitpunkt erstellter Snapshot, der es ermöglicht, einen reproduzierten Workload in einen früheren Zustand zurückzuversetzen.

Workload. Das Basis-Schutzobjekt in einer Datenablage. Ein Betriebssystem einschließlich dessen Middleware und Daten, das von der zugrunde liegenden physischen oder virtuellen Infrastruktur abgekoppelt ist.

Ziel. Ein Workload oder dessen Infrastruktur, der bzw. die das Ergebnis eines PlateSpin Protect-Befehls ist. Beispielsweise ist das Ziel beim anfänglichen Schutz eines Workloads der Failover-Workload im Container. In einem Failback-Vorgang ist es entweder die Original-Infrastruktur des Produktions-Workloads oder ein unterstützter Container, der von PlateSpin Protect inventarisiert wurde.

Siehe auch Ursprung.